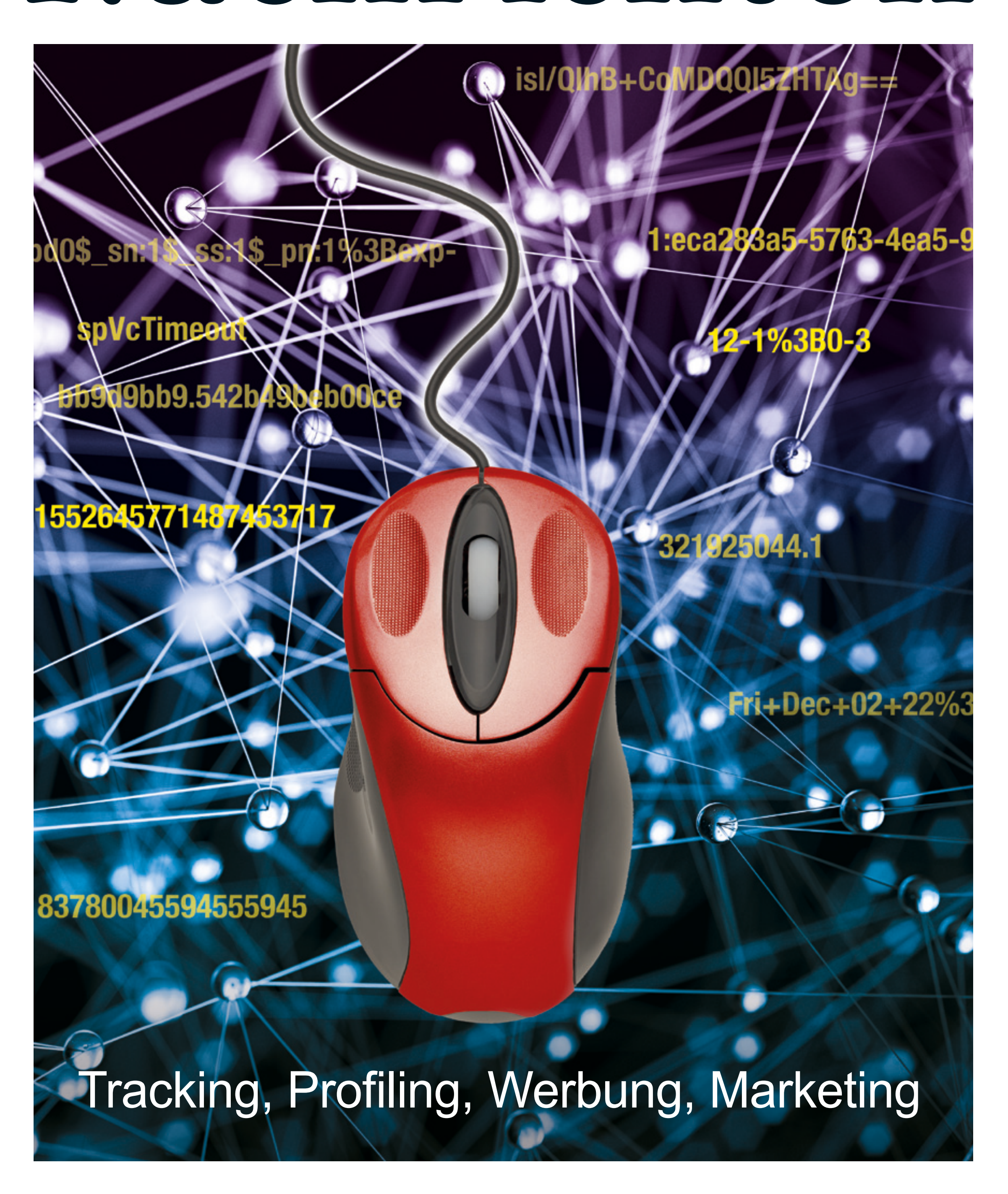
4/2016

Datenschutz Nachrichten

39. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Den Umsatz durch Tracking in einem Jahr verzehnfacht! ■ Was hilft gegen Online-Datensammler? ■ Kanzlerin besoffen mit den Datenkraken ■ Kommentare ■ Stellungnahmen ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Samstag, 28. Januar 2017
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Mittwoch, 01. Februar 2017
Redaktionsschluss DANA 1/2017
Thema: Verbraucherschutz

Dienstag, 21. Februar 2017
THM-Datenschutztag 2017
Campus Gießen, Gebäude B21.0.01 (Roxy Kino), Ludwigsplatz 4, 35390 Gießen
http://www.thm.de/datenschutz/veranstaltungen/thm-datenschutztag.html

Dienstag, 14. März 2017 und
Mittwoch, 15. März 2017
RKW-Bayern: Seminar zur Umsetzung der EU-Datenschutzgrundverordnung für betriebliche Datenschutzbeauftragte
München
http://rkwbayern.de/seminare-fachlehrgaenge/Veranstaltung/2547-seminar-die-datenschutzgrundverordnung-dsgvo-in-muenchen-17-115.html

Montag, 01. Mai 2017
Redaktionsschluss DANA 2/2017
Thema: BDSG-Nachfolgegesetz
alternativ Geheimdienste

Freitag, 05. Mai 2017, 18:00 Uhr
Big Brother Awards
Bielefeld, Hechelei
https://bigbrotherawards.de/

Sonntag, 21. Mai 2017
DVD-Vorstandssitzung
Berlin. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
39. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Werner Hülsmann, Frans Valenta
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta

Editorial

Eigentlich sollte diese Ausgabe ganz anders aussehen: Mehr Artikel zum Schwerpunktthema „Tracking, Profiling, Werbung, Marketing“. Aber es kam – wie so oft im Leben – anders. Am 22. November 2016 konnten wir die zweite – und zum damaligen Zeitpunkt noch nicht veröffentlichte – Version des „Datenschutzanpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)“ leaken. Nur einen Tag später kam die geringfügig veränderte offizielle Version mit einer sehr kurzen Frist zur Stellungnahme. Eine Darstellung der Entwicklung des BDSG-neu finden Sie im Artikel „Der holprige Weg zum BDSG-Nachfolger“. Auch unsere Pressemitteilungen und unsere Stellungnahme finden Sie aus aktuellem Anlass in dieser Ausgabe.

Als „Ausgleich“ gibt es in dieser Ausgabe daher nur drei Artikel und eine Buchbesprechung zum Schwerpunktthema. Ein weiterer Artikel beschäftigt sich mit einem Beitrag von Mikael Krogerus und Hannes Grassegger, der quasi „wie eine Bombe“ in die Datenschutzwelt einschlug. Zumindest wurde der Beweis erbracht, dass Big Data ohne Datenschutz unsere Demokratie gefährdet. Ob Trump seine Wahl auch ohne die Methode des Psychologen Michal Kosinski gewonnen hätte, wird sich nicht mehr feststellen lassen.

Wir wünschen Ihnen eine spannende und informative Lektüre.

Frans Valenta & Werner Hülsmann

Autorinnen und Autoren dieser Ausgabe:

Roland Appel

Jahrgang 1954, lebt und arbeitet als Unternehmensberater und Publizist in Bornheim / Rheinland, www.roaconsult.com und ist Mitherausgeber des „Datenschutz-Führerschein“ www.datenschutz-lernen.de. Von 1990-2000 war er Landtagsabgeordneter und Fraktionsvorsitzender der Grünen in NRW, Roland.Appel@RoaConsult.com.

Claus Egan

Fachmann für Datenschutz, Web-Analse, Web-Marketing und Social Media. Seit 2016 als externer Spezialist im Verimax-Team. Seine fachkritische Distanz zu Produkten oder Hypes hilft, den Blick auf den Marketingplan zu schärfen und sich auf die Unternehmensziele zurück zu besinnen, mail@verimax.de.

Werner Hülsmann

Vorstandsmitglied in der DVD, Mitglied des Beirats des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., selbständiger Datenschutzberater, externer Datenschutzbeauftragter und Datenschutzsachverständiger, Ismaning und Berlin, huelsmann@datenschutzverein.de.

Frank Spaeing

Externer Datenschutzbeauftragter, Vorstandsmitglied in der DVD, spaeing@datenschutzverein.de.

Stefan Staub

Geschäftsführer der Verimax GmbH und seit mehr als 20 Jahren Berater für Datenschutz und Informationssicherheit, mail@verimax.de.

Frans Valenta

Grafik- und Mediendesigner, Vorstandsmitglied in der DVD, valenta@datenschutzverein.de.

Dr. Thilo Weichert

Ehemaliger Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel, Vorstandsmitglied in der DVD, weichert@datenschutzverein.de.

Claus Egan, Stefan Staub

Den Umsatz durch Tracking in einem Jahr verzehnfacht!

Wer würde denn dazu *„Nein“* sagen wollen, noch dazu, wenn ein Werkzeug dafür sogar kostenlos angeboten wird!

Doch bei aller Euphorie, die solche oder ähnliche **Werbebotschaften** der Trackinganbieter ausstrahlen, tut man gut daran, die Sach- von der Werbeinformation, die tatsächlichen Fähigkeiten der Werkzeuge, den wirklichen Nutzen für das eigene Webprojekt und auch ein mögliches Schadenpotential sorgfältig gegeneinander abzuwägen. Schaden kann dabei künftig nicht nur auf der Seite der Betroffenen – also der Kunden – entstehen, sondern nunmehr durch die EU-DSGVO[1] in erheblichem Umfang auch auf der Unternehmensseite.

Datenschutzrechtliche Anforderungen sind hierbei nur ein Maßstab, ein anderer ist der effektive Nutzen bzw. Un-Nutzen für das Unternehmen selbst.

Für den sorgfältigen Abgleich ist es erforderlich, die Mechanismen, die im Webtracking-Markt existieren, zu kennen, um ihre Auswirkungen beurteilen zu können. So sollte man sich zunächst vor Augen führen, dass dieser Markt nicht ein-, sondern mehrdimensional ist. Es gibt nicht nur **eine** Anbieter- und **eine** Nachfrager-Ebene, vielmehr kann man in mindestens fünf solcher Ebenen unterscheiden:

1. Die Hersteller-Ebene

Es gibt mindestens mehrere Hundert Tracking-Technologie-Produkte am Markt, vom einfachen Seitenaufrufzähler bis zum hochkomplexen Multifunktionswerkzeug. Dementsprechend unterschiedlich ist auch der Preis: von (tatsächlich oder vermeintlich!) kostenlos bis zu jährlichen Lizenzkosten von mehreren Tausend Euro.

Dabei konkurrieren die Anbieter von lizenzbasierten Systemen nicht nur mit dem *Platzhirsch*[2] Google, sondern innerhalb des noch verbleibenden schmalen Marktsegmentes auch heftig untereinander.

Datenschutzaspekte werden künftig sicherlich besonders durch die **‚privacy by design‘**-Anforderungen der EU-DSGVO vorgegeben werden. Gerade die Hersteller sind zwar gefordert, eine datenschutzkonforme Konfiguration zu ermöglichen, sie werden das Risiko aber erfahrungsgemäß weitgehend an die Anwender weiterreichen.

2. Die Werbevermarkter-Ebene

Hier stehen große, multinational agierende Agenturen, die insgesamt sehr große Werbebudgets betreuen, im harten Wettbewerb zueinander. Selbst kleine Effizienzsteigerungen bedeuten für diese Agenturen nicht nur einen Wettbewerbsvorteil, sondern haben durch die Größe der Budgets auch erhebliche Auswirkungen auf den Ertrag.

Bei einigen dieser Anbieter verschwimmen die Grenzen zur Hersteller-Ebene, weil sie entweder eigene Systeme entwickelt haben und diese (inzwischen) auch vermarkten (Beispiel: Arvato) oder als Hersteller von einem Werbevermarkter gekauft wurden (Beispiel: Urchin Software Corp. im Jahr 2005 durch Google Inc.).

3. Die Agentur-Ebene

Dies sind Web-Dienstleister, die Tracking als ‚Messinstrument‘ für das Online-Marketing der von ihnen betreuten Websites empfehlen oder sogar vorschreiben. Dazu gehören nicht nur die klassischen Werbeagenturen, sondern z. B. auch sogenannte SEA[3]- oder SEO[4]-Dienstleister.

4. Die Anwender-Ebene

Dies sind die Website-Betreiber, die Tracking als ‚Messinstrument‘ für das Online-Marketing der eigenen Website nutzen. Im Gegensatz zur Werbevermarkter-Ebene ist die Anwender-Ebene jedoch der Hauptadressat der Werbung der Hersteller-Ebene.

5. Die Nutzer-Ebene

Die Besucher der Website, deren Nutzungsdaten erhoben und verarbeitet werden, also die (potentiellen) Kunden der Anwender-Ebene.

Inwiefern der Nutzer bzw. der Betroffene von den zukünftigen Anforderungen des europäischen Datenschutzrechtes profitiert, muss sich in der praktischen Anwendung der EU-DSGVO und ihrer Durchsetzung noch zeigen.

Dabei sind in den Ebenen 1 - 4 jeweils eigene ‚Gesetzmäßigkeiten‘ zu beachten:

Mechanismen der Hersteller-Ebene

Aus der Sicht der Hersteller geht es (bis auf ganz wenige Ausnahmen) hauptsächlich

- um den Zugang zu Nutzerdaten zur Profilbildung oder
- um Lizenzeinnahmen oder
- um die Nutzerdaten zur Profilbildung und Lizenzeinnahmen oder
- um die Steigerung der eigenen Linkpopularität.

Um sich hier von Google oder den anderen Mitbewerbern abheben zu können, müssen daher stets neue *Features* auf den Markt gebracht werden. Diese folgen dabei sowohl den technischen Möglichkeiten (Speicherplatz wird immer billiger, die Rechenleistung der Tracking-Server und die Netzkapazitäten nehmen zu), als auch den Anforderungen einzelner Kunden. Sie werden aber – ganz unabhängig davon, ob diese vom Durchschnittsanwender überhaupt gebraucht werden – als Must-have im Markt beworben und platziert.

Ein Beispiel: Viele Anwender betrachten die Tracking-Zahlen einmal wöchentlich, monatlich oder noch seltener. Dabei bleibt es sogar meist nur beim Betrachten der Zahlen, d. h., es existiert beim Anwender kein implementierter Prozess, auf Grund dessen nach der Zahlenbetrachtung Maßnahmen ergriffen werden.

Moderne Tracker sind jedoch in der Lage, die Analyse-Daten in Echtzeit zur Verfügung zu stellen und deshalb wird „Realtime-Tracking“ als wichtige Eigenschaft von den Anbietern hervorgehoben, deren Produkte über diese Möglichkeit inzwischen verfügen.

Sonderfall Google

Google ist nicht nur wegen seiner Marktdominanz und seiner Rolle sowohl als Hersteller, als auch als Werbevermarkter ein Sonderfall. Google ist als Hersteller in der Vergangenheit auch nicht als Technologie-Treiber in Erscheinung getreten, sondern hat Entwicklungen des Marktes dann rasch adaptiert, wenn diese die Nachfrage zu Lasten des eigenen Marktanteiles zu verändern drohten.

Google bietet sein Analytics-Werkzeug ja nicht aus Großzügigkeit ohne Lizenzgebühren an. Um im Wettbewerb der Suchmaschinen – besser: der (Suchmaschinen-)Werbevermarkter – die Nase vorn behalten zu können, sollte der Google-Besucher möglichst relevante Treffer zu seinem Suchbegriff erhalten. Je weniger individuell ein Suchbegriff ist, desto schwieriger wird es, das treffendste Ergebnis zu präsentieren (meint die Suche nach *Kohl* den Politiker oder das Gemüse?). Neben den Suchmaschinen-eigenen Bordmitteln wie Informationsgewinnung aus bisherigen Suchanfragen oder aus bekannten Vorlieben, die in (den insbesondere eigenen!) Sozialen Netzwerken publiziert wurden, gibt es noch die Möglichkeit, die Rückkehrzeit zu messen, nachdem die Suchmaschine zur Suchtrefferseite verlassen wurde. Kehrt der Besucher nämlich nach sehr kurzer Zeit wieder zurück, liegt die Vermutung nahe, dass ihn das Ergebnis nicht sonderlich interessiert hat.

Noch besser ist es da aber, wenn der Besucher auf der besuchten Seite weiter beobachtet werden kann! Hier kann dann auch gemessen werden, welche Detailseite wie lange betrachtet wurde und, wenn eine Zielseite ebenfalls mit Google-Analytics getrackt wird, sogar ob ein externer Link verfolgt wurde.

Google war durch seinen Marktanteil und die damit einhergehende Implementation auf sehr vielen, insbesondere wichtigen, Websites daher schon sehr früh in der Lage eine *Customer-Journey* abzubilden, hat aber beispielsweise dieses Feature nicht als Alleinstellungsmerkmal vermarktet.

Vielmehr bietet Google-Analytics heute selbstverständlich auch eine Customer-Journey an, wobei Google – und das ist aus Datenschutzsicht besonders aufschlussreich – dazu selbst schreibt: „*We analyzed millions of consumer interactions through Google Analytics ...*“[5], wobei mit *consumer interactions* nicht die Suchanfragen auf Google gemeint sein können!

Gegen die Marktmacht von Google müssen schon kräftige (technologische) Geschütze in Stellung gebracht werden. Solche werden dann beispielsweise Marketing-Automation, virtuelles Eyetracking, Customer-Journey oder Heatmaps genannt, um nur einige herauszugreifen.

Auf die Sinnhaftigkeit solcher Mess- und Analysemethoden für die Anwender wird später noch eingegangen. In erster Linie sind das aber eben nur Produkteigenschaften, die das eigene vom Mitbewerberangebot abhebt.

Mechanismen der Werbevermarkter-Ebene

Diese Analytics-Markt-Teilnehmer sind eine treibende Kraft, wenn es darum geht, die Werkzeuge dahin weiterzuentwickeln, individuellere Profile zu bilden, genauere Vorhersagen machen zu können, schnellere Ergebnisse liefern zu können oder einfach nur die Performance zu steigern. Denn auf Grund der Größe der Werbebudgets sind bereits kleinste prozentuale Verbesserungen im Ergebnis relevant.

Wie groß der Effizienzdruck ist, lässt sich am Beispiel der Cookies ganz gut zeigen: Im Jahr 2010 haben nur ca. 3 % der Internetnutzer Cookies in ihrem Browser blockiert (zum Vergleich: Q4.2015 ca. 11%). Trotz dieses damals homöopathischen Anteils an Cookie-Verweigerern wurden (und werden!) Methoden wie Flash-Cookies, EverCookies oder Digital-Fingerprinting entwickelt und eingesetzt.

Als im Februar 2013 angekündigt wurde, dass der Firefox-Browser ab April 2013 in der Grundeinstellung Cookies von Drittanbietern blockieren werde, reagierte die Werbebranche umgehend: „*Diese Voreinstellung wäre ein **nuklearer Erstschlag** gegen die Werbebranche*.“[6]

Dabei muss man sich im Klaren darüber sein, dass die Werbevermarkter-Ebene kein grundsätzliches Interesse daran hat, dass Werbung als solche wirkungsvoller wird; es geht hier lediglich um den Wettbewerb untereinander. Denn würde man durch entsprechende Metriken den Anteil ineffizienter Werbung aus dem Henry-Ford-Zitat „*Ich weiß, die Hälfte meiner Werbung ist hinausgeworfenes Geld. Ich weiß nur nicht, welche Hälfte*.“ auf NULL reduzieren können, würden sich die Werbebudgets weitgehend kompensationslos halbieren. Daran hat die Werbebranche kein wirkliches Interesse.

Mechanismen der Agentur-Ebene

Tracking wird in der Regel von den Agenturen nicht als Dienstleistung verkauft. Vielmehr wird oftmals beim technischen Design der Site Google-Analytics einfach mit eingebaut, weil „*es ja kostenlos*“ ist.

Dort, wo Agenturen das Thema „Tracking“ aktiv bewerben, bestehen häufig (verprovisionierte) Beziehungen zu entsprechenden Anbietern oder die Agentur profiliert sich über eine Google Analytics certified partner-Auszeichnung oder die Agentur nutzt solche Werkzeuge selbst intensiv für ihre Dienstleistung, z. B. SEA- oder SEO-Agenturen.

Außerdem muss eine Agentur Zweierlei beachten: Zum Einen würde sie sich den Zugang zu einem erheblichen Teil des Marktes selbst versperren, wenn sie **aktiv** Google-Analytics ablehnt und zum Anderen benötigt die Agentur, wenn sie Tracking-Analyse als Dienstleistung anbietet, entsprechendes Know-how. Hier liegt es nahe, die Mitarbeiter auf das Produkt zu schulen, das die größte Verbreitung im Markt hat.

Ähnlich wie bei den Datenverarbeitern im Auftrag wird sich in Zukunft auch mehr denn je zeigen, wer die An-

forderungen der EU-DSGVO so umzusetzen weiß, dass er dem Anwender nicht nur datenschutzkonforme Rezepte bietet, sondern **mit ihm gemeinsam** zielgerichtete Lösungen erarbeitet. Eine bloße Beratung lässt den Anwender nämlich im entscheidenden Moment allein.

Agenturen, deren Tagesgeschäft ja die Werbung ist, heulen erfahrungsgemäß gerne mit der Meute, d. h., sie springen auf die Werbephrasen der Hersteller auf, auch um zu zeigen, dass sie up to date sind. Dabei garantiert das Kopieren einer Methode, die bei einem Großen angeblich zum Erfolg geführt hat – Nichts! Es sei nur an die Social-Media-Euphorie vor einigen Jahren erinnert, als große Agenturen den Trend der Zukunft prognostiziert haben und stolz verkündeten, dass Unternehmen wie VW oder P&G sich den neuen Medien zugewandt haben und TV und Print dem Untergang geweiht seien. Das Gegenteil ist bisher zu beobachten![7]

Mechanismen der Anwender-Ebene

Da die Anwender der Hauptadressat der Werbung der Anbieter sind, entsteht auf die Marketingabteilungen der Anwender ein entsprechender Einsatz- und Modernisierungsdruck, insbesondere wenn sich die Geschäftsführung auf einer Veranstaltung[8] das neueste Internetwissen geholt hat und den Marketingverantwortlichen fragt: „*Warum machen wir denn nicht ...*".

Ebenso häufig wird Tracking zwar eingesetzt, aber nicht bzw. kaum ausgewertet, weil „*es ja kostenlos ist, da schadet es nicht*".

Ein gutes Beispiel dafür ist eine Evaluation eines Trackingtools bei einem DAX-Unternehmen gegen das eingesetzte Google-Analytics. Dabei wurde festgestellt, dass das neue Programm nur einen Bruchteil der Seitenaufrufe zählte und daher nicht infrage kam. Bei genauerer Betrachtung stellte sich jedoch heraus, dass der auf der Seite implementierte *Börsenticker* durch eine fehlerhafte Einbindung von Google-Analytics jedesmal einen neuen Seitenaufruf erzeugte, selbst wenn nur der Ticker aktualisiert wurde, die tatsächliche Anzahl der Seitenaufrufe also bisher viel zu hoch *gemessen* wurde. Das wollte man aber dem Vorstand dann doch lieber nicht erklären!

Ein anderes Problem ist darin zu sehen, dass die Budgets für das Web-Tracking angesichts der vermeintlich kostenlosen Angebote oftmals viel zu klein sind, um brauchbare Ergebnisse zu liefern. Deswegen sind die Marketingabteilungen gut beraten, wenn sie der Geschäftsleitungsebene ein schlüssiges Konzept vorlegen.

Was Anwender beim Tracking-Konzept beachten sollten

Tracking ist ein *Messinstrument*, das ein Unternehmen dann zwingend nutzen sollte, wenn das Geschäftsmodell Internet-getrieben ist.

Dazu muss das Tracking in das Gesamt-Webmarketing-Konzept sorgfältig eingebunden werden, d. h., vor dem Einsatz eines Tracking-Tools ist zu prüfen, welche Effekte gemessen werden sollen und **wie auf die Messungen reagiert werden kann**.

Ein ausschließlich im Internet agierendes Unternehmen oder ein Unternehmen, das signifikante Umsätze über das Internet generiert, hat gänzlich andere Anforderungen an die Website-Metrik als ein Unternehmen, das nur eine Web-Visitenkarte betreibt.

In einem übertragenen Bild: In der Formel 1 erfassen hunderte Sensoren permanent Daten und senden sie an die Box. Dort werden diese nicht nur von einer Software in Echtzeit ausgewertet, sondern die Ergebnisse darüber hinaus noch von mehreren Technikern parallel beobachtet und bewertet.

Auch wenn Websites bei weitem nicht so komplex sind wie Formel-1-Boliden, es also meist möglich ist, Entscheidungen von der Software treffen zu lassen, ändert dies wenig an den einzuplanenden Ressourcen.

So kann ich bei einer Online-Zeitung ein Metrik-Tool einsetzen, das das Interesse der Leser an einem Startseiten-Teaser eines Artikels misst und den Teaser nach unten verschiebt oder gänzlich entfernt, wenn die *Interessiert-mich-Quote* unter einen bestimmten Wert fällt. Dadurch kann ein Online-Redakteur deutlich entlastet werden. Es wird aber weiterhin ein neuer Artikel für die entstehende Teaser-Lücke benötigt!

Kein Tracking ohne Konzept

Nur wenn die Auswertung von Besucherzahlen oder deren Bewegungen auf der Website dazu führen, dass

- an der Website Veränderungen vorgenommen werden (Performance- bzw. Usability-Verbesserungen) oder
- **Aktionen** des Website-Besuchers ausgewertet werden oder
- die Website sich auf Grund der Messungen automatisch selbst ändern kann

ist Tracking überhaupt notwendig. In all diesen Fällen ist der Aufwand aber nicht mit dem Tracking beendet, sondern er ist bereits vorher nötig (Fähigkeit der Selbststeuerung) oder ist nach dem Messen zu leisten.

Kostenloses Tracking gibt es nicht!

Als Unternehmer sollte man sich auch davor hüten, selbst dem Geiz-ist-geil-Werbeslogan zu erliegen: Kein Unternehmen[9] hat etwas zu verschenken. Auch vordergründig kostenlose Tools wie Google-Analytics haben ihren Preis: Hier wird mit dem *Öl des 21. Jahrhunderts bezahlt* – den eigenen Daten!

Außerdem wird bei *kostenlos* gerne übersehen: Die Kosten entstehen überwiegend vor dem Bildschirm!

Je wichtiger das Internet für ein Geschäftsmodell ist,

- desto qualifizierter muss die Person sein, die die Analysen durchführt,
- desto umfangreicher muss ein Analysetool eingerichtet und abgestimmt werden,
- desto öfter und intensiver müssen die Ergebnisse betrachtet und bewertet werden.

Mit Einarbeitung, Einrichtung, Fortbildung und Durchführung kommen da schnell ein bis drei Stunden pro Woche zusammen (bei großen Projekten ist das ein Vollzeitjob). Bei (nur!) 40 EUR/Stunde sind das schon Kosten zwischen 2.000 und 6.000 EUR/Jahr!

Dabei muss zusätzlich berücksichtigt werden, dass bei nur geringem wöchentlichem Zeitaufwand die Effizienz leidet: Man muss sich jedes Mal wieder in das Projekt hinein denken und in das Werkzeug einarbeiten. Ist es zusätzlich noch kompliziert, das Tool zu parametrisieren oder die Ergebnisse auszuwerten, erhöhen sich die Personalkosten rasch.

Nicht nur auf das Kosten-Nutzen-Verhältnis kommt es an

Selbst bei kleinen Projekten kommen also ein paar tausend Euro zusammen, die sich durch den Einsatz des Analysetools amortisieren sollten. Erreicht die Maßnahme das Ziel (Aufmerksamkeit, Bestellung, Kontakt)?

So könnte beispielsweise im Bestellprozess erkannt werden, dass ein erheblicher Teil der Besucher zwar den Warenkorb gefüllt hat, die Seite aber wieder verlässt, nachdem die Zahlungskonditionen gezeigt wurden. Hier könnte nun durch eine bisher nicht angebotene Zahlungsart die Anzahl der Bestellabbrüche signifikant vermindert werden. In der Praxis zeigt sich tatsächlich häufig, dass bereits mit kleinen Änderungen erhebliche Wirkungen erzielt werden können.

Nicht immer lässt sich die Frage der Amortisation jedoch so einfach beantworten wie beim Internet-Bestellprozess. Je früher der Kontakt eines potentiellen Kunden mit der Website stattfindet oder je intensiver eine Beratung nötig ist – z. B. im B-to-B-Umfeld – desto schwieriger wird die Erfolgseinschätzung oder gar -messung. Dann muss man sich aber im Vorhinein des Risikos bewusst sein, gegebenenfalls eine Maßnahme „zum Fenster hinausgeschmissen zu haben" (um im Bild von Henry Ford zu bleiben). Es nicht versucht zu haben, wäre aber der größere Verlust, es sei denn, man kann oder will sich das Risiko nicht leisten.

Darum ist es so wichtig, bereits vor dem Einsatz eine klare Strategie zu haben und die erforderlichen Ressourcen bereit zu stellen. Weder macht man einen nicht konkurrenzfähigen Motor durch eine Verdoppelung der Sensorenzahl zum Sieger, noch kann der leistungsfähigste Bolide gewinnen, wenn im Cockpit und an der Box nur Pfeifen sitzen. Insofern unterscheidet sich Web-Analyse auch nicht von einer Werbekampagne: Wer nicht in der Lage ist, Fernsehwerbung zu schalten, braucht kein Filmskript erstellen lassen!

Das Nutzen-Schaden-Verhältnis nicht außer Acht lassen

Gerne wird auch der Fehler gemacht, dass nur die unmittelbaren Lizenz- und Personalkosten bzw. Erträge (durch eine Steigerung des Bestelleingangs) betrachtet werden. Es gibt jedoch noch andere beeinflussende Faktoren, beispielsweise:

- Welcher Aufwand entsteht durch zusätzliche Datenschutz-Anfragen?
- Wie hoch ist das Risiko, abgemahnt zu werden?
- Sind Bußgelder aufgrund datenschutzrechtlich *unsauberer Implementierung* zu erwarten?
- Welcher Imageschaden kann entstehen?
- Wie viele Kunden gehen verloren, weil sie sich *ausspioniert* fühlen?

Gerade die letzte Frage ist deswegen interessant, weil sie die Grenzen der Online-Metrik aufzeigt: Es kann zwar gemessen werden, wie sich der Besucher auf der Website bewegt, es bleibt aber fast immer im Dunkeln, warum er die Seite verlässt. Gerne wird von *Online-Metrik-Fetischisten* ins Feld geführt wird, es sei wichtig, Besucher in Echtzeit identifizieren zu können. Denn, so die Argumentation, falls dieser eine konkrete Besuch zu einem erheblichen Umsatz führt, könne man daraus Maßnahmen für die Zukunft ableiten. Auf die Frage, wie man einen erheblichen Umsatzverlust, der durch die Website entsteht misst, bekommt man dann aber regelmäßig keine Antwort.

Sich nicht durch Werbebotschaften blenden lassen

Eine Reihe von Tracking-Tool-Features sind auf den ersten Blick vielversprechend, leisten aber in der Praxis nicht das, was man davon erwartet hatte.

Ein **Marketing-Automation-Tool** automatisiert nicht das Marketing, ersetzt nicht den Vertrieb und führt nicht automatisch zu mehr Ertrag. Dabei spricht nichts dagegen, die Vertriebsrelevanz einer Kontaktanfrage über die Website zu messen, um schnell auf jene reagieren zu können, die mit größerer Wahrscheinlichkeit zu einem Verkauf führen.

Vielleicht wäre es aber auch hilfreich, nicht bloß die pure Anzahl der durch die Website produzierten Leads zu steigern, sondern die Seite so zu gestalten, dass möglichst nur wirkliche Interessenten den Kontakt suchen.

Es mag ja zutreffend sein, dass Mausbewegungen beim Lesen einer Website mit den Augenbewegungen des Lesers korrelieren. Aber wie viele Menschen kennen Sie, die beim Besuch von Internetseiten die Maus als Lesehilfe benutzen?

Wenn **Eyetracking** für ein Webprojekt wirklich wichtig ist, wird man um eine sichere Ermittlung (mit entsprechenden Kosten) nicht herum kommen. Umgekehrt: Wenn diese Kosten zu hoch sind, ist Eyetracking nicht nötig, weil das Projekt nicht wichtig ist!

Eine der häufigsten Falschaussagen auf Websites lautet: „*Wir nehmen den Schutz Ihrer Daten besonders ernst*.". Gleichzeitig wird – ob absichtlich, durch Unkenntnis oder durch Bequemlichkeit – der *König* Kunde bespitzelt, was das Zeug hält.

Man stelle sich das Bild vor: Ein Marketingleiter besucht eine Messe und wird vom Eintritt an über verschiedene Messestände hinweg von einer Person verfolgt, die ihm bei jedem Gespräch schweigend über die Schulter schaut. Und wenn er die Person schließlich genervt fragt, was sie denn da tue, zur Antwort erhält: **Customer-Journey**!

Apropos Datenschutz und Tracking: manch deutscher bzw. europäischer Anbieter präsentiert sein Angebot gerne stolz als „*datenschutzkonform nach deutschem BDSG", „... nach EU-Recht*" oder „*Geprüft durch Hamburger Datenschutzbehörde*", um sich von der *Datenkrake* Google positiv abzuheben – verletzt aber selbst einfachste Datenschutzregeln. Warum sollte man ausgerechnet solchen Anbietern seine Daten und die seiner Kunden anvertrauen?

1 Europäische Datenschutz-Grundverordnung

2 mit einem Marktanteil von über 80 %

3 Search Engine Advertising

4 Search Engine Optimization

5 https://www.google.com/analytics/resources/gms-online.html

6 http://www.zdnet.de/88148884/firefox-blockiert-kunftig-cookies-von-drittanbietern/

7 http://www.wiwo.de/unternehmen/handel/werbesprech-milliarden-zum-fenster-hinauswerfen/14438072.html

8 http://www.bieg-hessen.de/blog/online-marketing/sanjay-sauldie-rockt-mit-seiner-keynote-die-preisverleihung-des-hessischen-website-awards-in-der-ihk-frankfurt-am-main/

9 Werkzeuge wie PIWIK aus der Open-Source-Community sind keine Angebote von Unternehmen! Wenn Sie es nutzen und nicht sponsern, hat eben ein Anderer die Entwicklungskosten für Sie bezahlt.

Frans Valenta

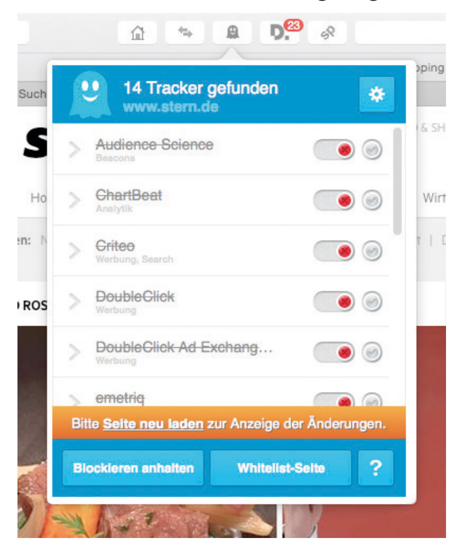
Was hilft gegen Online-Datensammler?

Angela Merkel verkündete am 16. November 2016 „Das Prinzip der Datensparsamkeit kann nicht die Richtschnur sein für die neuen Produkte". Sigmar Gabriel forderte eine Wende zu mehr „Datensouveränität" – in der Neusprech-Übersetzung: Verzicht auf Datenschutz.

Die fehlenden Reaktionen von vielen betroffenen Politikerinnen und Politikern[1] auf das Bekanntwerden der Nutzer-Datenweitergabe bei dem Browser-AddOn WOT (Web Of Trust)[2] zeigt, dass Datenschutz bei ihnen als unwichtig betrachtet oder gar als „Handelshemmnis" eingestuft wird. Die enge Verflechtung von Wirtschaft und Politik führt dazu, dass die Profit bringende Ausspähung der Bürger vor den Schutz der Privatsphäre gestellt und die Erfassung des Web-Nutzerverhaltens zur Kategorie „Neue Geschäftsmodelle im Internet" deklariert wird. In dem NDR-Beitrag „Nackt im Netz"[3], der die kommerzielle WOT-Datenweitergabe öffentlich gemacht hat, wird empfohlen, das AddOn direkt zu löschen.

„Daten sind die Rohstoffe des 21. Jahrhunderts" war eine der zentralen Aussagen von Kanzlerin Merkel kurz vor der Cebit 2015[4]. Mit Daten sollen sich demnach neue Einnahmequellen erschließen lassen. Dabei wird im „Neuland" Internet mit Daten als Ware schon eifrig experimentiert. Vor allem die Werbeindustrie möchte möglichst viel über die Internetnutzer erfahren, um „zielgerichtet" Werbung platzieren zu können. Daher gibt es inzwischen fast keine einzige Webseite mehr, die nicht zumindest Analysetools wie Piwik[5] einsetzt, um herauszufinden, wofür sich mögliche Kunden im Internet interessierten. Das quelloffene Piwik lässt sich bei entsprechender Konfiguration datenschutzkonform einsetzen. Wer Google Analytics einsetzt, handelt nach dem Grundsatz „Der Zweck heiligt die Mittel"[6]. Da Google nichts zu verschenken hat, möchte der Konzern an den Daten partizipieren und somit ist es praktisch unmöglich, dieses Instrument nach deutschen Datenschutzregeln so einzusetzen, dass die Persönlichkeitsrechte des Webnutzers gewahrt werden[7].

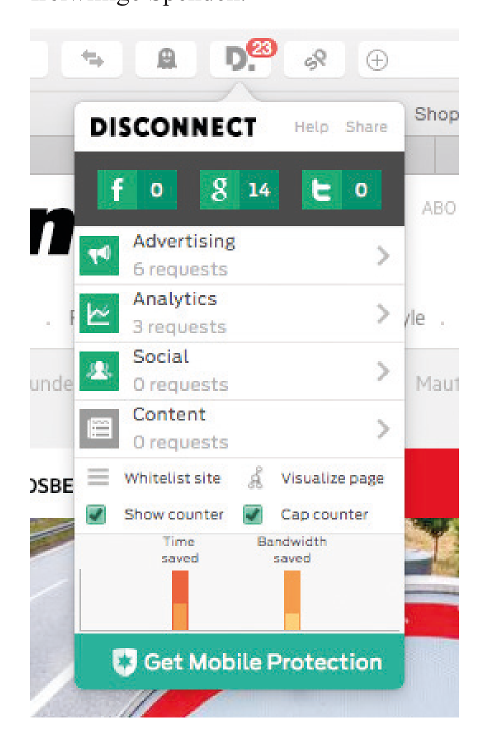
Natürlich möchte kein Internet-Nutzer bespitzelt werden. Deswegen benutzen die Werbe-Dienstleister möglichst unauffällige Werkzeuge – z. B. unsichtbare Minibilder (Zählpixel), Cookies oder Javascript-Tags. Gegen Zählpixel gibt es zumindest bei HTML-E-Mails einfache Möglichkeiten zum Schutz: Die Mail wird online abgerufen aber offline gelesen, die HTML-Funktion des E-Mail-Programms wird abgeschaltet oder die Darstellung externer Grafiken wird deaktiviert. Cookies sind leider in manchen Fällen nicht so einfach zu umgehen, denn einige Webseiten-Betreiber verwehren dann den Interessenten den Zugang – wie Springer mit bild.de. Der Verlag nutzt die Beliebtheit des Portals aus, um die Leser zu zwingen, ausgespäht zu werden. Nutzer, die Anti-Tracking-Tools wie Ghostery oder Adblock Plus verwenden, bekommen eine Seite zu sehen, in der sie aufgefordert werden, Adblocker zu deaktivieren. Anzeigenkunden können demnach hier sicher sein, dass ihre Scripts und Werbebanner bei den Bild-Lesern ankommen. Ghostery erfüllt zwar den Zweck der Blockier-Funktion und macht die Tracking-Aktionen durch Angabe der informationshungrigen Firmen und Netzwerke transparent, allerdings stellt der Hersteller seine Datenbank auch der Werbewirtschaft zur Verfügung[8], weshalb von einer Verwendung abgeraten wird. Eine Alternative wäre Adblock Plus, allerdings wird die Entwicklung des Programms aus der vom Oberlandesgericht Köln für illegal erklärten Acceptable-Ads-Initiative finanziert[9].



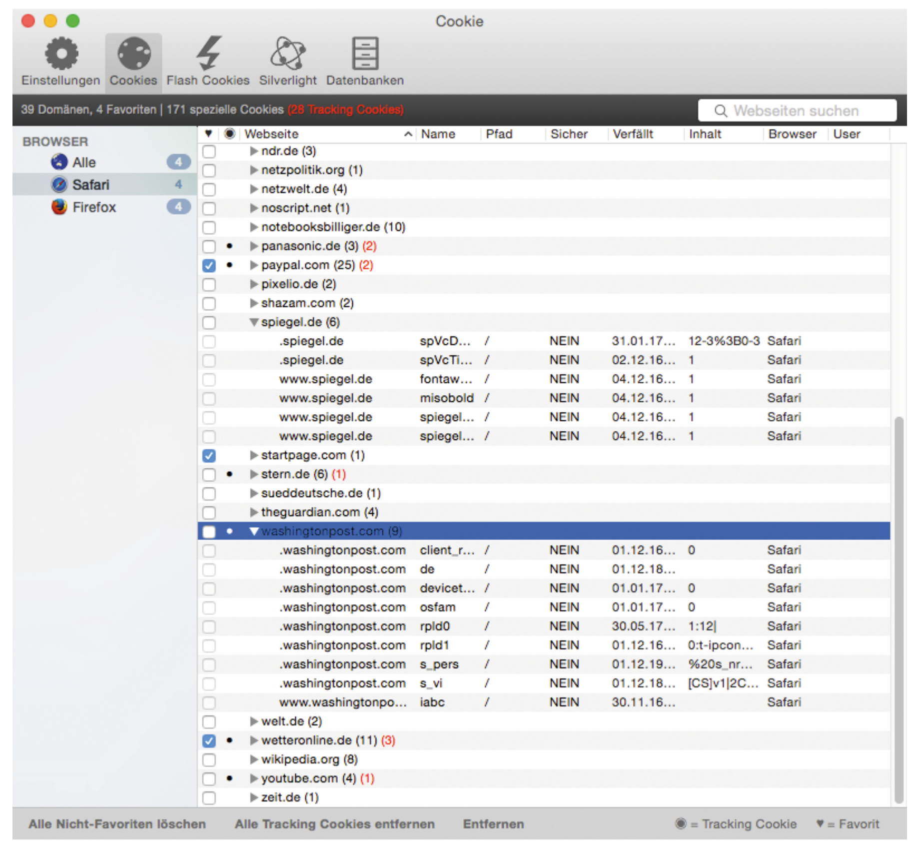


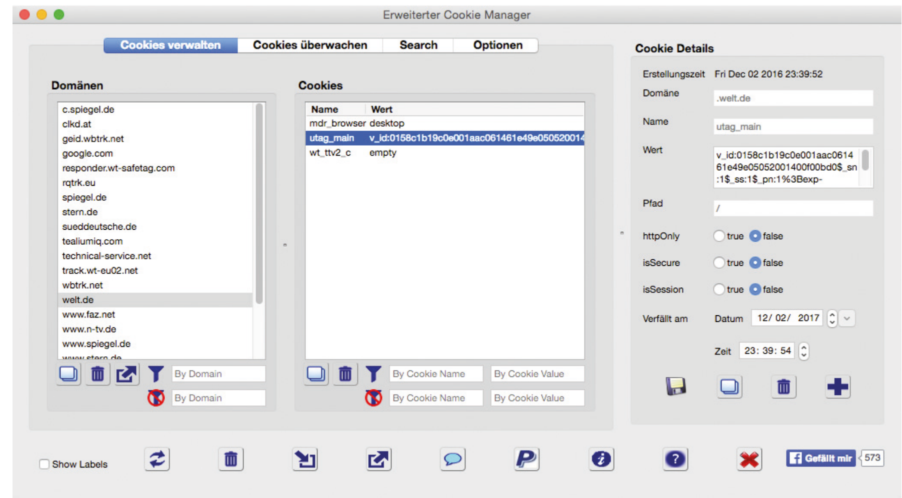
Noscript blockiert aktive Inhalte einer Webseite wie Java-Applets, JavaScript, Adobe Flash, Microsoft Silverlight und soll so gewährleisten, dass zumindest ein Teil der Tracking-Versuche scheitert. Mit JavaScript ist durch das Sammeln von System-Konfigurationen wie installierte Plugins und Schriftarten eine eindeutige Zuordnung des Rechners möglich (Browser-Fingerprinting)[10]. Ein Problem: Viele interaktive und/ oder animierte HTML5-

Seiten sind ohne JavaScript praktisch nicht darstellbar. Immerhin gibt es bei den Werkzeugen zur Tracking-Blockade auch eine vertrauenswürdigere Open-Source-Software: Disconnect[11]. Sie ist für alle Betriebssystem-Plattformen und fast alle Browser verfügbar. Die Entwicklungs-Finanzierung erfolgt über freiwillige Spenden.



Die für das Identifizieren und Verfolgen von Nutzern gesetzten Cookies lassen sich mit Abblockern nicht ausnahmslos ausfiltern, aber man kann sie mit spezialisierten Programmen auflisten und manuell löschen. Auf Mac-Computern stellt „Cookie“[12] dazu nützliche Funktionen bereit. Das für Safari und Firefox konzipierte eigenständige Programm zeigt auf einer Webseite erfasste Cookies mit Pfad, Namen, Sicherheit, Verfallsdatum und Inhalt an. Tracking-Cookies werden rot markiert dargestellt. Nützliche Cookies, die das lästige Abtippen immer wiederkehrender Werte ersparen, können als Favoriten deklariert werden und werden vom Löschen ausgenommen. Im Prinzip bietet fast jeder Browser die Möglichkeit, Cookies aufzulisten und zu löschen – wenngleich nicht immer besonders detailreich und komfortabel. Plattformübergreifend (Mac, Linux, Windows, iOS und Android) gibt es als Ergänzung für Firefox und Chrome „Cookie Manager“.

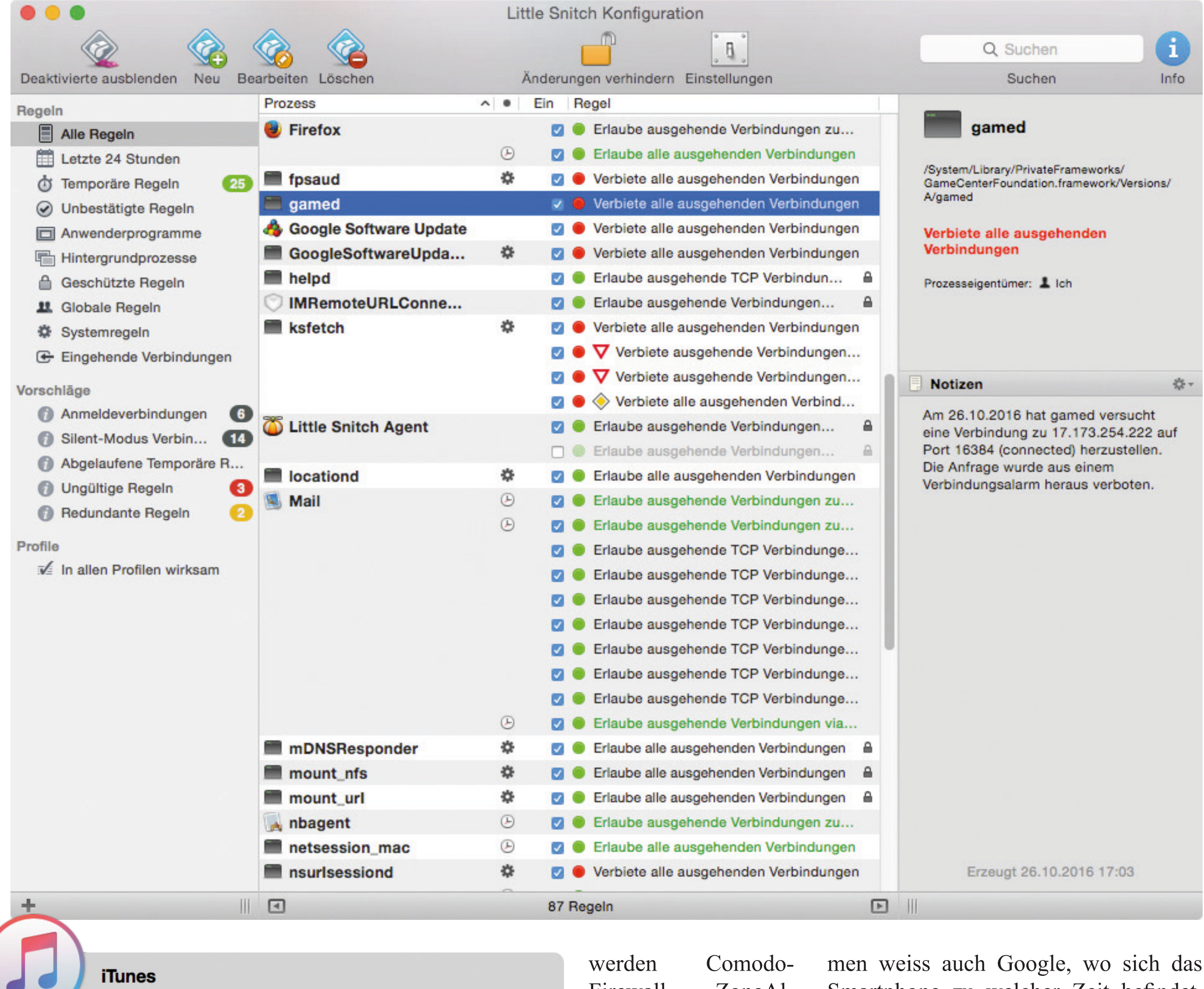




Die Darstellung von Cookie und Cookie Manager im Vergleich

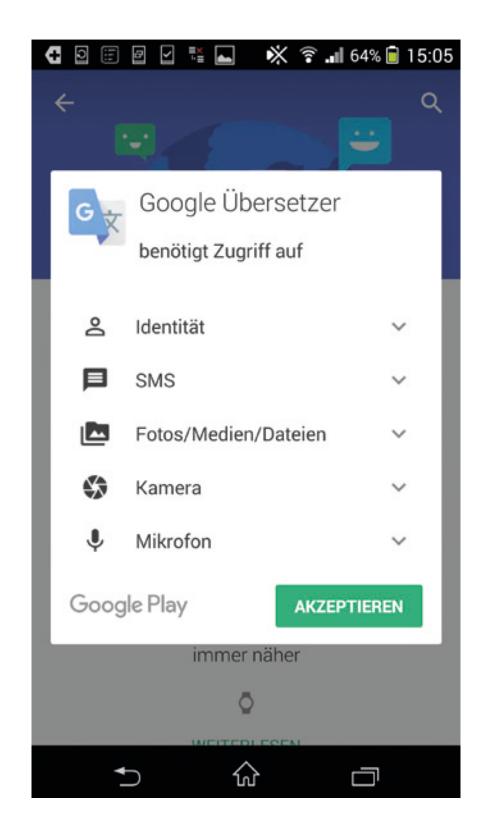
Das „Safebrowsing“ von Google soll Endanwender vor Phishing und Malware schützen. Es ist in Firefox, Chrome und Safari implementiert. Das Tool vergleicht die übertragenen Web-Adressen mit einer aktuelle Liste, zu der eine Verbindung mit Google aufgebaut wird. Wer sicher gehen möchte, dass keine privaten Daten nach außen kommuniziert werden, sollte diese Funktion abschalten. Auf der Webseite von Digitalcourage gibt es dazu ausführliche Beschreibungen[13].

Fast alle Tracking-Blocker verhindern innerhalb von Browsern, dass Daten erfasst und „nach Hause” gesendet werden. Aber was ist mit anderen Programmen, die Daten sammeln und weitergeben? Microsoft hat mit seinem Betriebssystem Windows 10 seinen Anwendern per Standardeinstellung eine umfassende Datenübertragung verordnet[14], die in vielen Fällen nicht erforderlich ist und deaktiviert werden sollte. Auch Apple verzichtet nicht darauf, Daten zu sammeln. Seit dem Betriebssystem Mac

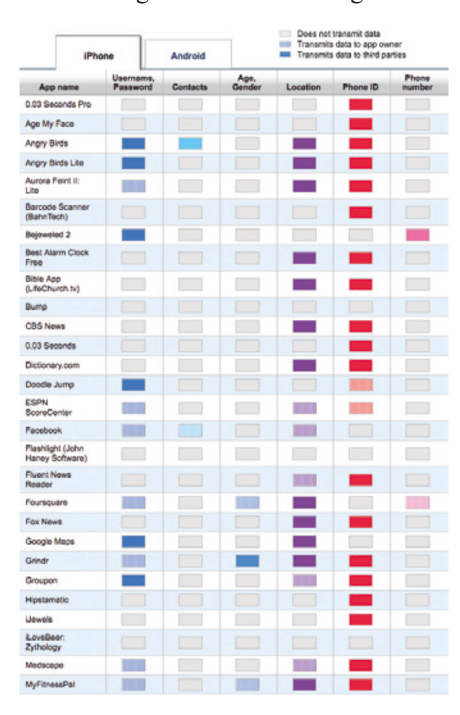


OS X 10.8 werden im Sekundentakt im Hintergrund für das Game-Center bestimmte Daten (gamed) an Apple-Server geschickt, unabhängig davon, ob der Dienst in Anspruch genommen wird oder nicht[15]. Mit einem Programm wie Little Snitch kann eine derartige Aktivität aufgespürt und nach vordefinierten Regeln ohne Beeinträchtigung der Funktionalität abgeschaltet werden[16]. Leider gibt es für Windows, Linux, iOS und Android keine vergleichbar komfortablen Lösungen. In der Windows-Welt werden Comodo-Firewall, ZoneAlarm und Windows 10 Firewall Control wohl noch am nächsten an die Leistungsfähigkeit von Little Snitch herankommen. Für Linux-Anwender käme Douane als Alternative in Betracht. Gerade für Android-Nutzer wäre ein vergleichbares Tool für den Online-Betrieb sehr nützlich. Leider sind die im Google PlayStore dazu angebotenen Apps nur rudimentär geeignet, ausgehende Verbindungen zu kontrollieren. Viele Apps beinhalten vorinstallierte Google-Dienste, z. B. das GPS-Tracking oder die Sprach-Eingabe. Alle Informationen werden von Google aufgezeichnet und können im Google-Konto unter „Meine Aktivitäten“ eingesehen werden. Bei der Benutzung von Navigationsprogrammen weiss auch Google, wo sich das Smartphone zu welcher Zeit befindet. Bewegungsprofile werden visuell dargestellt. Sprachanfragen bei der Suche im Chrome-Browser oder Diktate in Textverarbeitungsprogrammen werden als Audiodateien gespeichert. Und auch Suchanfragen im Browser oder Listen angeschauter YouTube-Filme sind detailliert rekonstruierbar.

Google stellt zur Zeit ca. 2,4 Millionen Apps im PlayStore zur Verfügung[17]. Viele Apps kosten noch nicht einmal 10,- Euro und es gibt eine Riesenauswahl kostenloser Programme. Da stellt sich die Frage, wie die Entwicklung und der Vertrieb finanziert wird. Die Antwort: Werbung und Daten. Die kostenlosen Apps blenden in der Mehrzahl zum Teil nervige Werbebanner ein. Das Programm bietet ein Upgrade zu einer kostenpflichtigen werbefreien Version an. Ob mit oder ohne Werbung – eine erschreckend hohe Zahl an Apps sammelt Daten und übermittelt



sie zum Teil an Dritte, wie aus einer Untersuchung von 101 beliebten Apps durch das Wallstreet Journal hervorgeht[18]. Vor der Installation von Apps gibt es seitens Google zwar Hinweise, auf welche Daten die Anwendungen auf dem Smartphone zugreifen, aber kaum ein Nutzer macht sich wirklich Gedanken darüber, welche Auswirkungen eine Zustimmung hat.



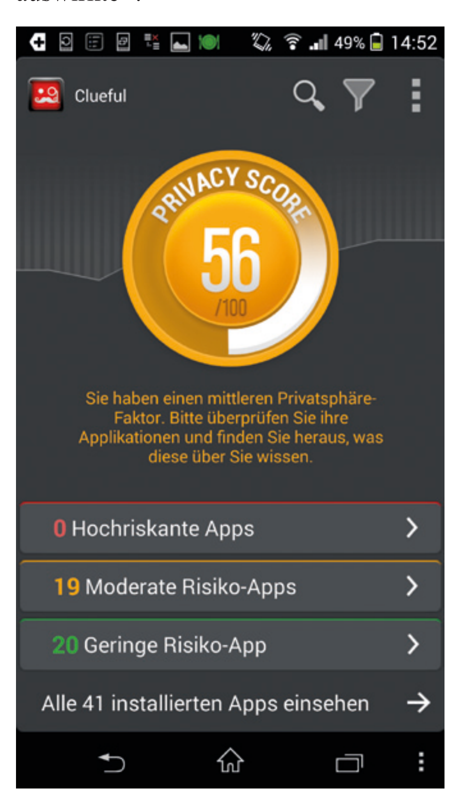
iPhone | Android

Does not transmit data
Transmits data to app owner
Transmits data to third parties

App name	Username, Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro						
Age My Face						
Angry Birds						
Angry Birds Lite						
Aurora Feint II: Lite						
Barcode Scanner (BahnTech)						
Bejeweled 2						
Best Alarm Clock Free						
Bible App (LifeChurch.tv)						
Bump						
CBS News						
0.03 Seconds						
Dictionary.com						
Doodle Jump						
ESPN ScoreCenter						
Facebook						
Flashlight (John Haney Software)						
Fluent News Reader						
Foursquare						
Fox News						
Google Maps						
Grindr						
Groupon						
Hipstamatic						
iJewels						
iLoveBeer: Zythology						
Medscape						
MyFitnessPal						

Screenshot einer Tabelle aus der Untersuchung des Wallstreet Journals

Auch wenn nicht alle Hersteller von ihren Möglichkeiten gebrauch machen, *„könnten 35,97 Prozent den Aufenthaltsort des Nutzers feststellen, während sie geöffnet sind. Bei 13,46 Prozent ließe sich die individuelle Geräte-ID hochladen, zum möglichen Anlegen eines Verhaltensprofils über mehrere Apps hinweg. 9,14 Prozent der Apps könnten Kontakte auslesen, 9,91 Prozent die Telefonnummer auslesen und auf Drittanbieter-Server hochladen, 6,43 Prozent die E-Mail Adresse hochladen und 6,65 Prozent den Browser-Verlauf auslesen“* geht aus einer Studie von Bitdefender hervor[19]. Das Unternehmen bietet Nutzern die kostenlose App „Clueful“[20] an, die anzeigt, wie die auf dem Smartphone installierten Programme mit datenschutzrelevanten Informationen umgehen. Die Software gab es auch schon mal für iOS, allerdings wurde sie von Apple aus dem AppStore entfernt – möglicherweise weil sie entweder zuviel über die Daten-Sammel-Gepflogenheiten des Konzerns in Cupertino verriet oder sich negativ auf bestimmte App-Downloads auswirkte[21].



Was wäre, wenn alle Internetnutzer durchgängig Adblocker und Software zur Verhinderung von ausgehenden Verbindungen einsetzen würden? Würden Werbetreibende dann wieder Werbung nach dem Gießkannenprinzip wie bei Printmedien einsetzen? Eher nicht – wahrscheinlich würden Lobbyisten das in der für sie üblichen Weise über die Politik regeln.

1 http://www.zeit.de/digital/datenschutz/2016-11/datenschutz-browser-erweiterungen-wot-bundestagspolitiker

2 https://netzpolitik.org/2016/datenhungrige-browserplugins-machen-politiker-erpressbar-und-bedrohen-journalismus/

3 http://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html

4 http://www.faz.net/aktuell/wirtschaft/cebit/vor-der-cebit-merkel-daten-sind-die-rohstoffe-des-21-jahrhunderts-14120493.html

5 https://www.datenschutzzentrum.de/tracking/piwik/20110315-webanalyse-piwik.pdf

6 https://www.google.de/intl/de/analytics/

7 https://www.datenschutzzentrum.de/presse/20110315-piwik.htm

8 https://www.ghostery.com

9 https://www.heise.de/newsticker/meldung/Klage-gegen-Adblock-Plus-Teilerfolg-fuer-Springer-Niederlage-fuer-Eyeo-bei-Acceptable-Ads-3248585.html

10 https://panopticlick.eff.org/about

11 https://disconnect.me

12 https://sweetpproductions.com

13 https://digitalcourage.de/blog/2016/wot-addon-google-safe-browsing

14 http://www.verbraucherzentrale.de/windows10

15 http://www.blog-it-solutions.de/mac-os-game-center-telefoniert/

16 http://www.blog-it-solutions.de/mac-os-netzwerk-internet-ueberwachen/

17 https://de.statista.com/statistik/daten/studie/74368/umfrage/anzahl-der-verfuegbaren-apps-im-google-play-store/

18 http://blogs.wsj.com/wtk-mobile/

19 http://www.bitdefender.de/news/bitdefender:-android-apps-verzichten-auf-das-ueberfluessige-sammeln-von-user-daten-2776.html

20 http://www.bitdefender.de/solutions/clueful-android.html

21 https://techcrunch.com/2013/05/21/after-getting-booted-from-apples-app-store-mobile-privacy-app-clueful-returns-on-android/

Roland Appel

Kanzlerin besoffen mit den Datenkraken

Der jährliche IT-Gipfel der Bundesregierung 2016 legte einen Wettlauf der Politik und Wirtschaftsinteressen um den vermeintlichen „Datenschatz" offen, der sich gegen die Bürgerrechte und jeglichen Datenschutz richtet. Die Kanzlerin polemisierte unsensibel und mit ungewohnt wenig Sachkenntnis gegen die verfassungsrechtlichen Prinzipien der Zweckbindung und Datensparsamkeit – Eckpfeiler des modernen Datenschutzes. Industrielle Partner der Regierung verrieten, wie die Große Koalition ein zentrales Bürgerportal mit Personenregister für alle Bürger errichten will, in dem die Steuernummer zum zentralen Personenkennzeichen würde. Das ist nicht nur unter dem Aspekt der liberalen Freiheitsrechte problematisch. Der eigentliche Irrtum der GroKo liegt darin, dass sie die Gefahren für die Gesellschaftsordnung und die soziale Marktwirtschaft völlig unterschätzen, die von der Digitalisierung ausgehen. Politik muss die Gefahren der Digitalisierung für Demokratie und soziale Gerechtigkeit erkennen und handeln, um Populismus zu bekämpfen.

Goldgräberstimmung der Datenindustrie

„Wir sind ja hier unter uns" meinte Karl-Heinz Streiblich, Vorstandsvorsitzender der Software AG kürzlich auf einer Veranstaltung des diesjährigen „IT-Gipfels" der Bundesregierung in Saarbrücken. Schauplatz war eine der Insiderveranstaltungen, zu denen sich jährlich etwa tausend Lobbyisten von Microsoft, Google, Facebook, SAP und Co. und Regierungsmitglieder von der Kanzlerin über die Bildungsministerin bis zum Justiz- und zum Wirtschaftsminister unter Ausschluss der Öffentlichkeit und weitestgehend ohne Journalisten und demokratische Öffentlichkeit in den Armen liegen. Datenschützer haben zu diesem Branchenauflauf traditionell keinen Zutritt, obwohl hier viel über Datenschutz geredet wird – zumeist abfällig. Und im Jahr vor der Bundestagswahl wollten die Großkoalitionäre, ob Kanzlerin, Dobrindt, Gabriel oder Wanka offensichtlich den Boden für die vermeintliche „Goldgräberstimmung" der Datenkraken bereiten, wie wir sie bereits seit Jahren aus den USA kennen.

Geradezu losgelassen polemisierten „Key-Note Speaker" gegen den Datenschutz als vermeintliches Hindernis eines gigantischen Wirtschaftswachstums. Allen voran Kanzlerin Merkel, die sich mit schillernden, aber nichtssagenden Begriffen wie „Gigabit-Zeitalter", „digitalem Binnenmarkt" und „Datensouveränität" an sich selbst nahezu besoffen redete. Sie lobte zunächst die sinnvolle zentrale Erfassung der Asylbewerber in einem Verbundsystem des BAMF, um dann sogleich eine rechtsstaatlich unanständige Parallele zu den „schon immer hier lebenden" Bundesbürgern zu ziehen. Diese sollten, so Merkel, „Teil eines Kerndatensystems werden" und „wir müssen schon eine kleine Bewegung schaffen, dass die seit langem in unserem Land lebenden Bürger dies auch wollen." Sprich: Merkel möchte gerne das vom Bundesverfassungsgericht verbotene allgemeine Personenkennzeichen für alle Bundesbürger einführen. Durch die Hintertür eines Serviceportals. Ein kleiner Schritt für Merkel, aber ein großer Schritt für den Überwachungsstaat!

Ein Personenkennzeichen hintenrum

Ein bürgerfreundliches Portal zu errichten, auf dem vom Bafög über die Kfz-Ummeldung bis zur Beantragung des Kindergeldes alle Stellen erreichbar sind, wäre durchaus an sich eine gute Sache. Allerdings könnte der Weg, wie dies umgesetzt werden soll, möglicherweise massiv mit der Verfassung kollidieren. Vom Chef der Software AG wurde der besondere Knaller benannt, mit dem man das bewerkstelligen wolle: durch die Zusammenführung der ELSTER-Daten des Finanzamtes, der verfassungsrechtlich umstrittenen Steuernummer als Personenkennzeichen mit denen des neu zu einzurichtenden personalisierten Datenportals. Steuernummer und Daten des Melderechts als Selbstbedienungsladen für die Datenwirtschaft? Kaum zu glauben.

Und weil die Kanzlerin kurz vor der Bekanntgabe ihrer erneuten Kandidatur offenbar so richtig in Fahrt und von keinen bürgerrechtlichen Bedenkenträgern gebremst war, verstieg sie sich gleich noch zur Feststellung, dass das Prinzip der Datensparsamkeit, Bestandteil der EU-Datenschutzgrundverordnung, „in Zeiten von Big Data wohl nicht die Leitschnur für die Entwicklung neuer Produkte sein könne". Und: Auch die Rechtsprechung müsse das begreifen. Naja, Bürgerrechte kamen ja im politischen Unterricht des „realen Sozialismus" nicht vor und belasteten auch nicht die Bundesregierungen unter Kohl, die den Großen Lauschangriff und die Vorratsdatenspeicherung beschlossen und in denen Merkel ihre politische Lehrzeit hatte. Wie schon bei der Ausspionierung ihres eigenen Handys durch die NSA machte Merkel auch in Saarbrücken wieder deutlich, dass zu ihrem Staatsverständnis nicht gehört, die Privatsphäre ihrer Bürger gegen die kommerziellen Interessen von Google und Co. zu schützen.

Große Koalitionen schaden den Bürgerrechten

Wer nun glaubt, dass etwa der SPD-Justiz- und Verbraucherschutzminister Heiko Maas derartigen verfassungsrechtlichen Ungereimtheiten Einhalt gebieten oder sich zumindest kritische Anmerkungen geleistet hätte, sieht sich getäuscht. Der kleine Mann aus dem Saarland blieb stumm. Dafür kommen

aus Sigmar Gabriels Ministerium seit Monaten die Töne eines Referenten für „Datenschutz“, der gebetsmühlenartig und gegen jede Verfassungswirklichkeit wiederholt, die Prinzipien der „Datensparsamkeit“ und der „Zweckbindung“ seien einfach in Zeiten von „Big Data“ nicht mehr zeitgemäß. Recht hat der Mann – wofür brauchen wir gegenüber Facebook und Google, Microsoft und Amazon, NSA und FBI, die jetzt bald von Donald Trump kontrolliert werden, noch irgendwelchen Datenschutz?

So könnte das Grundrecht, welches das Bundesverfassungsgericht 1983 geradezu hellseherisch formuliert hat, in der Tat in Bedrängnis geraten. Denn auch die Gerichte, das erwähnte die Bundeskanzlerin ausdrücklich in ihrer „Gipfelrede“, sollten in Zukunft „anders Recht sprechen“, damit man „im Gigabyte-Zeitalter“ mit Daten neue „Produkte“ schaffen könne. Nach den Zockern der Finanzindustrie nun die Zocker der Personenverdatung? Hat Frau Merkel nichts daraus gelernt, dass es im Internet immer wenige große Konzerne wie Microsoft, Google, Facebook, Ebay, Amazon oder Uber sind, die sich zu Oligopolen und Monopolen entwickeln und gigantische Profite machen? Und wer hat entschieden, dass wir auch in Europa eine solche Herrschaft der Datenkraken wollen? Die datenbesoffene Kanzlerin könnte sich allerdings verfassungspolitisch geirrt haben: Ist doch das Grundrecht auf informationelle Selbstbestimmung direkt aus Artikel 1 des Grundgesetzes, der Menschenwürde, abgeleitet. Und dieser Artikel darf in seinem Wesensgehalt nicht angetastet werden. Gut, zu Zeiten des Volkszählungsurteils hat sie noch in der DDR als Physikerin gearbeitet. Trotzdem: Wer die Kanzlerin auf dem IT-Gipfel in ihrer Wurschtigkeit gegenüber Datenschutz erlebt hat und angesichts der Alternativlosigkeit ihrer Kandidatur 2017 kann einem schon um die Bürgerrechte bange werden. Vielleicht sollte sich die eine oder andere Wählerin angesichts dessen doch noch einmal überlegen, ob es Alternativen zur GroKo gibt.

Es geht nicht nur um liberale Freiheitsrechte

Wo heute noch Polizei und Staatsanwaltschaft richterliche Entscheidungen benötigen, um auf Einwohnerdaten, Steuerdaten oder Konten zuzugreifen, könnte künftig vieles virtuell verknüpfbar sein. Man kann daran fühlen: Bürgerinnen und Bürger werden in der digitalen Welt vom Staat immer stärker als ein analoges Sicherheitsrisiko wahrgenommen, nicht nur als potenzieller Terrorist, sondern auch in vielen Bereichen der Daseinsvorsorge. All dies wird jedoch mit dem schönen Wort von der „Bürgerfreundlichkeit“ und dem „smarten“ Staat verbrämt. Ob die Bürger, wenn sie die Wahl hätten, mit einem freundlichen Verwaltungsangestellten direkt zu sprechen, statt sich virtuell über unendliche anonyme Behördenflure zu klicken, dies überhaupt wollen, wird gar nicht erst gefragt.

Apropos Sicherheitsrisiko: Donald Trump, Brexit und andere Populisten – Politikwissenschaftler analysieren, dass diese unter anderem deshalb im Aufwind sind, weil die Regierungen die „kleinen Leute“ weder gegen die Machenschaften der Finanzindustrie, noch gegen Verlagerung und Vernichtung von Arbeitsplätzen, gegen die Flüchtlingskrise, gegen die Interessen der Wirtschaft in Sachen Braunkohleverstromung, gegen das Schummeln von VW und Co. bei den Immissionen oder gegen die Aushöhlung des Rentensystems beschützen. Nun will Merkel noch auf einem weiteren Feld die Interessen der Bürger preisgeben. Gegenüber der „Big-Data-Industrie“, die sich in vielerlei Gestalt der persönlichen Daten der Bürger und damit deren persönlicher Freiheitsrechte bemächtigen möchte. Die Reaktion derer, die sich nicht mehr vom Staat beschützt, sondern ausgeliefert fühlen, wird auf dem Fuße folgen. Viel Spaß beim „weiter so“ – wir sehen uns bei den nächsten Wahlen!

Der Datenkapitalismus und die politische Krise

Es wäre zu kurz gegriffen, allein auf die Gefährdung der liberalen Freiheitsrechte abzustellen, um die es natürlich geht. Es geht daneben auch um eine tiefgreifende ökonomische Transformation des Kapitalismus, die ungebremst zu mehr Monopolen führen wird als wir uns heute erträumen. Ein Beispiel dafür ist Ebay – heute die weltweit beherrschende Verkaufsplattform für Privatleute und Händler. Die Beiträge von Ebay zum Umweltschutz durch die Eröffnung des weltweit größten Flohmarkts für Gebrauchtwaren seien hier ausdrücklich lobend erwähnt. Gleichwohl hat Ebay in den ersten 10 Jahren seiner Existenz nahezu alle nationalen, regionalen und mittelständischen Plattformen dieser Art verdrängt, aufgekauft oder in den Ruin getrieben. Das ist keine kapitalistische Boshaftigkeit, sondern systemimmanent bei der Bildung von Portalen im Internet, die eine Vielzahl von Akteuren auf einem Wirtschaftsplatz zusammen bringen – irgendwann wird es ein Monopol.

Das Internet fördert – siehe Google und Facebook – Monopole und Vorherrschaft und dieses Prinzip muss die Politik begreifen und sich dem im Interesse von Wettbewerb und ökonomischer Chancengleichheit entgegen stellen. Diese Freiheitsgarantie, die Wettbewerb für neue Marktteilnehmer ermöglicht, ist die neue, wichtigste Funktion des Staates in der Informationsgesellschaft. Das haben Merkel, Gabriel und ihre Parteien überhaupt nicht begriffen. Eigentlich entspricht das einer sozialen und zugleich wirtschaftsliberalen Denkweise, in der Stresemann, Erhardt und Helmut Schmidt standen. Der soziale und liberale Rechtsstaat steht heute gegenüber der informatisierten Wirtschaft vor gravierenden Herausforderungen, auch seine Rolle als Schutzmacht für Wettbewerb und Chancengleichheit in der Wirtschaft neu zu verorten und zwar für eine soziale Marktwirtschaft und für die Grundrechte des Individuums. Stellt sich die Politik dieser Herausforderung nicht und lässt sie einen ungezügelten Kapitalismus zu, besteht die Gefahr, dass sich Arbeitsverhältnisse, sozialer Zusammenhalt und gesellschaftliche Bindungen weiter zerrütten und das politische System weiter dem Populismus preisgeben. Ob Merkel hierzu den Mut hat, ist zu bezweifeln, weil es eine wirklich politisch (nicht parteipolitisch) linke, soziale und liberale Politik erfordern wird, diese Probleme zu lösen.

Digitale Anschläge gegen den sozialen Zusammenhalt

Asoziale Geschäftsmodelle wie der Taxidienst Uber sind ein extremes, aber auch gutes Beispiel für das, was ein

ungezügelter Datenkapitalismus anrichtet, wenn Regierungen und Rechtsstaaten ihre Funktion zum Schutz der Bürger vor Ausbeutung nicht wahrnehmen. In Deutschland hat der Staat nicht zugelassen, dass die aus guten Gründen für die Sicherheit der Fahrer und Fahrgäste bestehenden Regulierungen und Gesetze, die Mindeststandards an Ausbildung sowie behördlicher Registrierung lizensierter Taxifahrer durchgesetzt wurden. In vielen Ländern, die ihre Taxifahrer weniger beschützt haben, hat Uber inzwischen hunderttausende von kleinen Unternehmen vernichtet und Menschen arbeitslos gemacht. Aber auch andere Geschäftsmodelle wie das autonome „Google-Auto" würden allein in New York, wenn sie sich durchsetzten, über 300.000 Arbeitsplätze von Taxifahrern vernichten. Die Auswirkungen des digitalen Wandels müssen auf den Tisch, gesellschaftlich diskutiert und politisch entschieden werden. Weder Merkel noch Gabriel haben die politische Brisanz erkannt.

Die Finanzindustrie erwirtschaftet weiter mit Wetten und Zockereien auf irreale, nicht von ökonomischen Gegenwerten gedeckten Papieren, Derivaten und Aktien exorbitante Gewinne, denen keine reale Wirtschaftskraft entspricht. Sie schafft eine latente und digitale internationale Dauerkrise. Dieselbe Finanzindustrie möchte den Bürgern mit unseriösen Argumenten wie angeblichem Terrorismus und Geldwäsche mittelfristig die Freiheit des Bargelds rauben, um damit jede Form von wirtschaftlicher Tätigkeit zu kontrollieren und einen ökonomischen Orwell-Staat zu errichten. Abschaffung des Bargeldes als Zahlungsmittel gäbe jeder Bank, jedem Staat zu jedem Zeitpunkt und an jedem Ort der Welt die Möglichkeit, einzelne Menschen durch die Sperrung ihrer Konten ökonomisch und existenziell zu vernichten und gegenüber den Massen durch die Abhängigkeit aller von ihren Banken jede überzogene „Gebühr" durchzusetzen. Angesichts dieser Entwicklung nimmt die Bundesregierung nicht etwa Partei für die Rechte der Bürger, sondern Wolfgang Schäuble stößt in das Horn der Banken und verbrämt das mit angeblicher Bekämpfung von Korruption.

Die digitale Bedrohung der Presse als „vierte Gewalt"

Google und Facebook, aber auch Null-Lohn-Geschäftsmodelle wie die „Huffington Post" sind eine Gefahr für den gerecht bezahlten und unabhängigen Journalismus, der unverzichtbar für die demokratische Willensbildung ist. Journalismus, der unabhängig recherchiert, darf nicht durch nicht bestätigte, subjektive Berichte von Privatleuten, Betroffenen und parteiischen Beobachtern ersetzt werden. Die Existenz der klassischen Medien, Zeitungen und Zeitschriften ist weltweit in einer existenziellen Krise. Auf der Seite der Rezipienten fördern soziale Medien durch selektive Nachrichtenzuteilung aufgrund der gewonnenen Nutzerprofile und der verwendeten Algorithmen nicht den Dialog, sonder die Vertiefung von Gegensätzen. Sie leisten wichtige Beiträge zur Bestärkung extremistischer, terroristischer und zum Teil faschistoider Weltbilder. Von Donald Trump bis zum Ku-Klux-Klan profitieren in den USA schlichte und gewaltbereite Gemüter von den sozialen Netzen und Medien. Die ernsten Auswirkungen dieser Strategie erleben wir heute im Verhalten der AfD-Anhänger und Populisten in Europa, die sich mit Gerüchten und Halbwahrheiten hochschaukeln und unabhängige Medien als „Lügenpresse" diffamieren. Auch der IS und andere religiöse Extremisten profitieren von den sozialen Medien. Sie bekommen angeboten, nur das zu konsumieren, was ihr absurdes, zum Teil rassistisches Weltbild bestärkt. Der dramatisch wachsende Beitrag dieser Medien zur politischen Wirklichkeit weltweit ist Entsolidarisierung und Destabilisierung vor allem der Demokratien – das muss in jede Diskussion über digitale Risiken und Chancen Eingang finden.

Das ging im Datenrausch des IT-Gipfels 2016 völlig unter. Politik, Wissenschaft und Wirtschaft zeigten sich konzeptionslos gegenüber den existenziellen demokratischen Gefährdungen der allumfassenden Digitalisierung.

Überwachte Bürger im digitalisierten Verkehr

Während sich die Autokonzerne mit den Datenschützern auf Mindeststandards beim vernetzten Fahrzeug verständigt haben, sind es inzwischen vor allem die sogenannten „Drittanbieter", allen voran die Autoversicherer, aber auch wieder Google und Facebook, Stromerzeuger und Zulieferer, Parkhausbetreiber und Hotelportale sowie die Werbeindustrie, die Autofahrer und Fahrzeug beim „autonomen Fahren" und vernetzten Fahrzeug ausspionieren wollen. Sie gieren nach den Navigationsdaten, um Bewegungsprofile zu erstellen, um z. B. Entertainment oder Navigationshilfen zu verkaufen, wollen Informationen über Fahrverhalten gewinnen, um Versicherungstarife anzupassen oder Gewährleistungsansprüche abzuwehren und sie suchen nach Möglichkeiten, um Mobilitätsprofile der Fahrer für Werbung zu nutzen. Dabei stehen Zweckbindung und Datensparsamkeit dem Profitinteresse im Weg. Dass es gerade das sozialdemokratisch verantwortete Wirtschaftsministerium ist, das hier den ideologischen Türöffner spielt und die informationelle Selbstbestimmung der Bürger an ökonomische Interessen verschenkt, knüpft an eine unselige sozialdemokratische Tradition an, die von Noske bis zur Aushöhlung des Grundrechts auf Asyl reicht.

Einen Beitrag zum „Thema verfehlt" lieferte kürzlich Verkehrsminister Dobrindt, indem er nicht etwa einen Gesetzentwurf zum „autonomen Fahren" präsentierte, sondern einen solchen, der die zahlreichen Fahrzeugdaten sowie Insassenüberwachung erfasst, drei Jahre speichert und die Verfolgung von Geschwindigkeitsübertretungen und anderen Delikten so erleichtert. Nicht die Kernrisiken des „autonomen Fahrens" werden geregelt, die darin bestehen, dass geklärt werden muss, wer – menschlicher Fahrer oder der Automat – gefahren ist und dies eigentlich nur 30 Sekunden vor und nach einem potenziellen Unfall. Stattdessen will Dobrindt die Erfassung und Speicherung von Verhaltensdaten der Fahrer und Insassen – eine lupenreine Lobbyauftragsarbeit ohne Rücksicht auf Bürgerrechte.

Smarte Technik, gläserne Konsumenten, rechtlose Mitarbeiter, Arbeitsplatzvernichtung

Amazon, Lieferportale von Zalando bis Lieferando, Rewe und Edeka wollen die Daten der Konsumenten erlangen,

um ihnen rund um die Uhr personalisierte und auf ihre Konsumentenprofile zugeschnittene Warenangebote machen zu können, von denen die Zielgruppen heute noch nicht wissen, dass sie sie morgen kaufen wollen könnten. Dabei kommen ihnen die Stromkonzerne zu Hilfe, die mit dem „intelligenten Kühlschrank“, der weiss, wann Butter zur Neige geht, die Milch ranzig wird und neue bestellt, Big Data befeuern. Dass die Transporter der Versandhändler Innenstädte verstopfen und mit ihren Dieselmotoren zur Feinstaubbelastung der Metropolen beitragen, ist egal. Dass die Arbeitsverhältnisse bei Amazon und bei Paketdienstleistern mit einem Heer von Scheinselbständigen, mit immer mehr prekärer Beschäftigung einher gehen, Gewerkschaften immer zahnloser werden, hatte auf den Veranstaltungen des IT-Gipfels, den ja auch die SPD verantwortete, keine Stimme. Wichtige Zukunftsfragen wurden auf dem IT-Gipfel nicht gestellt – sie erfordern aber politische Konsequenzen:

- Wollen wir wirklich „Smart Cities“, in denen energiesparende LED-Straßenlaternen zu WLAN-Stationen werden, die unsere Smartphones mit Internet versorgen und dafür unsere Bewegungs- und Aufenthaltsdaten gewinnen und speichern? Dass sie mit Videokameras ausgestattet eine umfassende Überwachung des öffentlichen Raumes ermöglichen?
- Wollen wir wirklich, dass unter dem Thema E-Health der Kontakt mit Ärzten oder Psychologen auf den Bildschirm reduziert und damit ein ganz essenzieller Teil der Kommunikation für z. B. Kassenpatienten auf dem Land abgeschafft und direkte Betreuung den besserverdienenden Privatpatienten vorbehalten bleiben?
- Glauben wir wirklich, für die Wirtschaft 4.0 ausreichend gerüstet zu sein, während Auszubildende und Mitarbeiter über keine Kenntnisse von Datensicherheit und Datenschutz verfügen, während die Wirtschaftsspionage von China und Russland, von NSA und CIA dem Maschinenbau, dem Mittelstand und der Industrie zusetzen?
- Glauben wir an die Versprechungen der angeblichen Umweltfreundlichkeit der E-Mobilität angesichts der Tatsache, dass die PKWs lediglich 14% des CO²-Ausstoßes verursachen, während immer noch ein großer Teil des Stroms aus Braunkohlekraftwerken mit 35% Wirkungsgrad erzeugt werden?
- Wollen wir, dass die Umstellung auf Elektromobilität in Stuttgart, München, Ingolstadt und Wolfsburg rund hunderttausend Arbeitsplätze der Motor-, Getriebe- und Hinterachsproduktion kosten würde? Können wir den Apologeten der Umweltfreundlichkeit der E-Mobilität wirklich vertrauen, obwohl Ladung, Betrieb und Wartung jede Menge Daten über Benutzer erheben werden, die Entsorgung der ökologisch problematischen Lithium-Batterien völlig ungeklärt ist und datensparsame Möglichkeiten zur Ladung der Fahrzeuge von der Industrie bisher völlig vernachlässigt werden?

Dr. Axel Friedrich, lange Jahre Abteilungsleiter Verkehr beim Umweltbundesamt, den Sigmar Gabriel in seiner Zeit als Umweltminister zu entlassen versucht hat, sagt dazu: „Baut endlich kleine, leichte, umweltfreundliche Autos mit modernsten kleinen Verbrennungsmotoren mit Hybridunterstützung. Die Technik ist vorhanden und wird uns ermöglichen, in den kommenden 20 Jahren wirklich effiziente und ökologische Antriebe zu entwickeln.“

Digitale Vernunft statt digitaler Drogenrausch

2017 könnte ein wichtiges Datum für eine Zeitenwende werden. Die Politik beschäftigt sich scheinbar mit der Bekämpfung von Populismus, Trump, AfD, Marine Le Pen oder Geert Wilders, ohne einsehen zu wollen, dass deren politische Erfolge viel mit den Problemen zu tun haben, die sie selbst in Form einer weltweite rücksichtslosen Umverteilung von unten nach oben und rücksichtsloser Geschäftsmodelle ohne gesellschaftliche Verantwortung geschaffen hat wie Sozialabbau, verfallende Infrastruktur und prekäre Beschäftigungsverhältnisse. Bezeichnend für die Entsolidarisierung des von Konrad Adenauer und Ludwig Erhard geschlossenen Paktes zwischen Arbeitgebern und Arbeitnehmern und der Generationen ist die aktuelle Rentendiskussion, die heute allein auf die Generationenfrage abstellt und diese gegeneinander ausspielt. CDU und FDP blenden die Verantwortung der Unternehmen für die Rente völlig aus und wenden sich damit gegen katholische Soziallehre und soziale Marktwirtschaft. Sozialminister Ehrenberg in der Regierung Helmut Schmidt forderte 1976 bereits eine „Maschinensteuer“, um alle Schichten am gesellschaftlichen Produktionszuwachs teilhaben zu lassen. Aus gutem Grund. Die Tatsache, dass digitale Techniken die Treiber von Innovation und Produktivität sind, muss von der Politik beachtet werden. Alle angeführten gesellschaftlichen Entwicklungen haben mit Digitalisierung zu tun. Sie sind krisenhaft und Krisen erzeugend. In allen Fällen bietet die Digitalisierung keine Lösung, sondern lediglich eine Verstärkung der jeweiligen Tendenz des Problems. Die Digitalisierung der Gesellschaft ist kein Selbstzweck. Sie ist ein Instrument. Sie kann helfen, Probleme umfassender zu verstehen. Sie kann aber auch helfen, Probleme zu verschleiern. Die Menschen in politischer Verantwortung müssen das erkennen und daraus Wege entwickeln, die die Probleme von Arbeitsplatzvernichtung, immer ungerechterer Einkommens- und Chancenverteilung, Konzentration von Kapital, Macht und Datenherrschaft und sozialer Ungerechtigkeit bekämpfen. Sie dürfen sich nicht fasziniert und kritiklos zum Helfer der Wirtschaftsinteressen machen – zum Beispiel durch die Aufhebung der Prinzipien von Datensparsamkeit und Zweckbindung.

Frank Spaeing

Von Bomben, Big Data und Präsidentschaftswahlen

Wie ein Artikel die deutschsprachige Internetwelt erst sehr aufgerüttelt und dann zu intensiven Diskussionen angeregt hat.

Am 3.12.2016 veröffentlichte Das Magazin aus der Schweiz den Artikel „Ich habe nur gezeigt, dass es die Bombe gibt" von Hannes Grassegger und Mikael Krogerus auf seiner Webseite[1]. In diesem Artikel schreiben die Autoren, wie der polnische Forscher Michal Kosinski – sein Schwerpunkt bei der Forschungsarbeit ist die *„Psychometrik, ein datengetriebener Nebenzweig der Psychologie"* – am Wahlmorgen, dem 9.11.2016, sich die Frage stellt, ob er für den Wahlerfolg Donald Trumps verantwortlich ist. Im Verlauf des Artikels wird ausgeführt, wie der Forscher feststellt, dass Ergebnisse seiner Forschungsarbeiten scheinbar das englischen Unternehmen Cambridge Analytica zu einem Produkt geführt haben, von dem der CEO Alexander James Ashburner Nix behauptet, dass dieses Produkt Donald Trump zum Wahlsieg verholfen habe.

Durch Zuordnen von Internetnutzern in bestimmte psychologische Kategorien in Kombination mit den Datenbergen, die von besagten Internetnutzern durch Big-Data-Technologien in sozialen Netzwerken wie Facebook gesammelt werden, könne man Verhalten und Einstellungen ziemlich exakt vorhersagen: *„2012 erbringt Kosinski den Nachweis, dass man aus durchschnittlich 68 Facebook-Likes eines Users vorhersagen kann, welche Hautfarbe er hat (95-prozentige Treffsicherheit), ob er homosexuell ist (88-prozentige Wahrscheinlichkeit), ob Demokrat oder Republikaner (85 Prozent). Aber es geht noch weiter: Intelligenz, Religionszugehörigkeit, Alkohol-, Zigaretten- und Drogenkonsum lassen sich berechnen. … Bald kann sein Modell anhand von zehn Facebooks-Likes eine Person besser einschätzen als ein durchschnittlicher Arbeitskollege. 70 Likes reichen, um die Menschenkenntnis eines Freundes zu überbieten, 150 um die der Eltern, mit 300 Likes kann die Maschine das Verhalten einer Person eindeutiger vorhersagen als deren Partner. Und mit noch mehr Likes lässt sich sogar übertreffen, was Menschen von sich selber zu wissen glauben."*

Fazit des Artikels ist, dass das Mutterunternehmen vom Cambridge Analytica, die amerikanische Firma SCL – Strategic Communications Laboratories, welche nach eigenen Aussagen eine Wahl-Management-Agentur ist, die mit Hilfe von *„Marketing auf Basis eines psychologischen Modells"* Wahlbeeinflussung ermöglicht. Und so Trump zum Sieg verholfen und die Engländer in den Brexit getrieben haben, indem sie die Wähler, die von der Gegenseite nicht überzeugt waren, davon abgehalten haben zu wählen und die eigene Kernwählerschaft jeweils im großen Umfang mobilisiert haben.

Auch ich habe diesen Artikel gelesen und war erst einmal verstört, habe ihn an Kollegen und Freunde weitergeleitet und mit diesen diskutiert.

Aber dann kam ziemlich schnell die Gegenbewegung im Internet. Denn der Artikel hat große Wellen geschlagen. Von Spiegel Online (in der Kolumne von Sascha Lobo)[2] bis zur Süddeutschen Zeitung[3] brachten diverse Medien Beiträge über diesen Artikel. Und diese betrachteten das Thema durchaus differenzierter.

So kommt die Süddeutsche zu dem Fazit: *„Wenn Wahlentscheidungen sich immer weiter Konsumoptionen angleichen, stecken darin politische Risiken, kein Zweifel. Aber gerade die multioptionalen Bedingungen der pluralistischen Gesellschaft könnten auch die Grenzen der politischen Manipulation sein. Einfacher gesagt: Wir kaufen ja auch sonst nicht alles, was uns Anzeigen anbieten."*

Sascha Lobo spricht vom magischen Digitalismus, der Tatsache, dass wir mittlerweile Algorithmen magische Fähigkeiten zuzuschreiben. *„Der magische Digitalismus aber wird zum doppelten Problem der Gesellschaft. Einerseits, wenn dieser Digitalaberglaube aus Unwissen entsteht, und andererseits, wenn er aus der Hybris, der Selbstüberschätzung der Wissenden entsteht."* und *„Der magische Digitalismus dagegen bietet tolle gefühlte Digitalerklärungen und versperrt so den Blick auf Kausalzusammenhänge."*

Auch in dem WDR-Blog[4] wird anhand vieler weiterführender Referenzen der ursprüngliche Artikel intensiv diskutiert und viele seiner Aussagen werden entkräftet oder relativiert.

Aber es bleibt trotzdem ein komisches Gefühl. War der ursprüngliche Artikel jetzt nur eine Art Marketing-Veranstaltung für das englische Unternehmen? Oder wird es in Zukunft doch potentiell große Probleme mit Big Data und Wahlen geben, so wie Herr Caspar in der Augsburger Allgemeinen schrieb?[5]

Wir werden die nächsten Wahlen in Europa mit wachem Blick verfolgen müssen, wir müssen sicherstellen, dass wir nicht selbst an der Verbreitung von Fake News teilhaben, nicht dem magischen Digitalismus verfallen. Und es ist sicher weiterhin eine gute Idee, immer mal wieder die Frage zu stellen, ob wir die Menge der Daten, die wir im Zweifelsfall unbedarft von uns preisgeben, nicht beschränken können und wollen.

1 https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

2 http://www.spiegel.de/netzwelt/web/magischer-digitalismus-wie-unser-technik-aberglaube-uns-allen-schadet-a-1124836.html

3 http://www.sueddeutsche.de/digital/facebook-targeting-vor-us-wahl-was-hinter-der-angst-vor-big-data-steckt-1.3287648

4 https://blog.wdr.de/digitalistan/hat-wirklich-der-grosse-big-data-zauber-trump-zum-praesidenten-gemacht/

5 http://www.augsburger-allgemeine.de/politik/Datenschuetzer-warnen-vor-Big-Data-im-Wahlkampf-id39922602.html

Werner Hülsmann

Entwurf der ePrivacy-Verordnung ist öffentlich – Auswirkung auf das Direktmarketing?

Nachdem am 10. Dezember 2016 darüber berichtet[1] wurde, dass der Entwurf der Nachfolgeregelung der ePrivacy-Richtlinie von der EU-Kommission am 11. Januar 2017 in Brüssel vorgestellt werden soll und es sich bei dieser Nachfolgeregelung um eine direkt wirkende Verordnung handeln wird, wurde am 13. Dezember der Entwurf[2] der ePrivacy-Verordnung (ePrivVO) geleakt.

An dieser Stelle kann noch keine umfassende Stellungnahme zu dem Entwurf erfolgen. Eine für viele Unternehmen wichtige Fragestellung soll hier aber bereits beleuchtet werden:

Das elektronische Direktmarketing

Relevant ist hierbei vor allem Art. 16 ePrivVO-E, in dem die bisherige Regelung aus Artikel 13 ePrivacy-Richtlinie übernommen wird. Diese Regelung wurde bislang in Deutschland (in völlig unpassender Weise) im § 7 des Gesetzes gegen den unlauteren Wettbewerb umgesetzt. In Art 16 Abs. 2 ePrivVO-E finden sich die (in Deutschland durch § 7 Abs. 3 UWG umgesetzten) Regelungen zur vereinfachten Erlaubnis zur Nutzung von E-Mail-Adressen (oder SMS-Nummern) für eigene Werbezwecke, wenn die dortigen Bedingungen (s.u.) erfüllt sind.

Diese Beibehaltung bestätigt die bereits vertretene Auffassung, dass sich die insbesondere der Satz „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." aus Erwägungsgrund 47 der EU-Datenschutzgrundverordnung (DSGVO) zum Direktmarketing nur auf das postalische Direktmarketing, nicht aber auf das Direktmarketing per elektronischer Kommunikation (E-Mail, Telefon, FAX, SMS) bezieht.



Wesentliche Punkte des Entwurfs ePrivVO

Die folgende Darstellung ist nur eine erste kurze Einschätzung und verzichtet auf den (wesentlichen) Teil der Verordnung, der nur für die Unternehmen gilt, die Dienste der elektronischen Kommunikation für die Öffentlichkeit anbieten:

- Art. 1 Abs. 3 ePrivVO-E: Die ePrivVO konkretisiert und detailliert die Regelungen DSGVO, insoweit in der ePrivVO die Verarbeitung personenbezogener Daten geregelt ist.
- Art. 4 Abs. 1 ePrivVO-E: Die Begriffsbestimmungen aus der DSGVO gelten auch für die ePrivVO.
- Art. 4 Abs. 2 lit f und g: Hier sind die Definitionen von „electronic mail" und „direct marketing communication" enthalten.
- Art. 9 ePrivVO-E: Nach Art. 9 Abs. 1 ePrivVO-E gelten für Einwilligungen die Anforderungen aus Art. 7 DSGVO.
- Art. 16 Abs. 1: ePrivVO-E: Werbung mit Hilfe elektronischer Kommunikation (E-Mail, Telefon, AX, SMS) ist nur mit vorheriger Einwilligung der End-Nutzer zulässig.
- Art. 16 Abs. 2 ePrivVO-E: Enthält die Regelungen der bereits bekannten vereinfachten Erlaubnis für Werbung für „electronic mail" bei Einhaltung der dortigen Regelungen (Erhebung der Daten bei Verkauf einer Ware oder Dienstleistung in Übereinstimmung mit der DSGVO, Werbung für eigene ähnliche Produkte und Dienstleistungen, Hinweis auf die werbliche Nutzung sowie Hinweis auf Widerspruchsmöglichkeit bei Erhebung und bei jeder Nutzung).
- Art. 25 ePrivVO-E Abs. 4: Die Mitgliedstaaten sollen die Sanktionen für Verstöße gegen Art. 16 (und andere Artikel) der ePrivVO selbst regeln.
- Art. 31 ePrivVO-E, Inkrafttreten und Anwendbarkeit: Das Inkrafttreten ist am 21. Tag nach der Verkündung im EU-Amtsblatt vorgesehen, gelten soll die Verordnung sechs Monate nach dem Inkrafttreten.

Eine ausführlichere Bewertung des – bis dahin dann offiziell bekannt gemachten – Verordnungsentwurfs wird in einer der nächsten DANA-Ausgaben erfolgen.

Fazit

Mit dem Entwurf der ePrivacy-Verordnung wird das Verhältnis zwischen der EU-Datenschutzgrundverordnung und den bereichsspezifischen Regelungen zum Datenschutz in der elektronischen Kommunikation deutlich besser geregelt als es noch mit der ePrivacy-Richtlinie möglich ist. Es bleibt allerdings abzuwarten, welche Entwicklung der jetzt bekannt gewordene Entwurf im Rahmen des EU-Gesetzgebungsverfahren erfahren wird.

1 https://dsgvo.expert/entwurf-fuer-die-nachfolgeregelung-der-e-privacy-richtlinie-wird-am-11-januar-2017-vorgestellt/ oder kürzer: https://dsgvo.expert/rN93E

2 http://www.politico.eu/wp-content/uploads/2016/12/POLITICO-e-privacy-directive-review-draft-december.pdf

Frank Spaeing

Der holprige Weg zum BDSG-Nachfolger

Eine Beschreibung der ersten Etappen aus Sicht der DVD

Im September 2016 hat das BMI als das federführende Ministerium einen ersten Entwurf eines Gesetzes zur Umsetzung der Europäischen Datenschutz-Grundverordnung (DSAnpUG-EU) an ausgewählte Ministerien und u.a. auch die BfDI zur Stellungnahme übersandt. Im Vorfeld hatten schon diverse Organisationen und auch Einzelpersonen Anforderungen an den Nachfolger des im Mai 2018 durch die Europäische Datenschutzgrundverordnung (DSGVO) in Teilen obsolet werdenden Bundesdatenschutzgesetzes (BDSG) aufgestellt. Auch die DVD hatte in Zusammenarbeit mit digitalcourage eine „Position zur Ausgestaltung der Europäischen Datenschutzgrundverordnung" (u.a. in der DANA 2/2016[1]) veröffentlicht[2]. Dieser erste Entwurf, der wie so oft vor der offiziellen Veröffentlichung geleakt wurde[3], wurde nach teilweise substantieller Kritik[4] gar nicht erst offiziell in die Verbändeanhörung gegeben. Im November kam dann wieder Bewegung in den Gesetzgebungsprozess, ein zweiter Referentenentwurf machte die Runde. Dieses Mal war es die Deutsche Vereinigung für Datenschutz e.V. (DVD), die als erste den zweiten Entwurf (mit Stand vom 11.11.2016) eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vorab veröffentlichte[5]. Im Folgenden die Pressemitteilung der DVD zum geleakten Entwurf[6]:

Datenschützer kritisieren neuen BDSG-Referentenentwurf

Das Bundesministerium des Innern (BMI) hat einen zweiten Entwurf eines Gesetzes zur Umsetzung der Europäischen Datenschutz-Grundverordnung (DSGVO) vorgelegt, den die Deutsche Vereinigung für Datenschutz e.V. (DVD) exklusiv veröffentlicht. Die DVD hält auch diesen Entwurf für massiv verbesserungsbedürftig. Ein erster Entwurf vom September war umgehend zurückgezogen worden, nachdem er von fast allen Seiten heftig kritisiert worden war. Nach Ansicht der DVD ist der jetzt vorgelegte Entwurf gesetzestechnisch besser gelungen. Dies gilt für die in Deutschland traditionell bestehende Aufteilung zwischen Datenschutz im öffentlichen und im nicht-öffentlichen Bereich, für die Systematik sowie für die Bezugnahmen auf die DSGVO. Doch enthält der Entwurf nach der Ansicht der DVD alte und teilweise auch neue europarechts-und verfassungswidrige inakzeptable Regelungen. Dies gilt für die Beschränkung der Kontrollbefugnis der Datenschutzaufsichtsbehörden auf technischeAspekte bei Berufsgeheimnisträgern wie z. B. Ärzten, Psychologen und Anwälten. Dringend nötige Regelungen zum Schutz der Berufsgeheimnisse unterbleiben dagegen. Die Einschränkungen des Auskunftsanspruchs der Betroffenen – der „Magna Charta des Datenschutzes" – mit Argumenten der Sicherheit sowie des Schutzes von Betriebs-und Geschäftsgeheimnissen verletzt das verfassungsmäßige Grundrecht auf Datenschutz. Bei den materiellen Regelungen versucht das BMI eine vom Bundesgesetzgeber noch gar nicht verabschiedete Vorschrift zur Videoüberwachung nach Wirksamwerden der DSGVO fortzuschreiben, mit welcher Sicherheitsbelangen der Vorrang vor dem Datenschutz eingeräumt wird und für die der nationale Gesetzgeber überhaupt keine Regelungsbefugnis hat. Nicht akzeptabel sind für die DVD insbesondere auch die Beschränkungen der Prüf-und Berichtsbefugnis der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im Geheimdienstbereich und die Beschränkung der Sanktionsmöglichkeiten der BfDI in den Bereichen Polizei und Justiz. Parallel dazu wird der BfDI die Vertretungsbefugnis Deutschlands im Europäischen Datenschutzausschuss (EDSA) auch für den nichtöffentlichen Bereich eingeräumt, obwohl sie bisher nur im Bereich der Post-und Telekommunikationsunternehmen Prüfkompetenz und Erfahrungen hat. Die Unabhängigkeit der Landesdatenschutzbeauftragten wird durch Verfahrensregeln beeinträchtigt, wie z.B. zu der Bestellungsbefugnis der Stellvertreterfunktion im EDSA durch den Bundesrat.

Frank Spaeing, Vorsitzender der DVD, kritisiert: „Der Entwurf ist eher ein Datenschutzverhinderungsgesetz. Das Bundesjustiz- und Verbraucherministerium, das Bundeswirtschafts- sowie das Bundesforschungsministerium müssen unbedingt umgehend intervenieren, da die Zeit für eine rationale Gesetzgebung in dieser Legislaturperiode ausläuft und grundlegende verfassungsrechtliche Notwendigkeiten sowie die Belange von Wirtschaftsunternehmen, Verbrauchern und Forschung ignoriert werden." Thilo Weichert, Vorstandsmitglied der DVD, ergänzt: „Die Einschränkung der Datenschutzkontrolle im ärztlichen Bereich, die bisher ein Schwerpunkt der Aufsichtsbehörden ist, ist schlichtweg eine Katastrophe. Es ist kaum zu glauben, dass in Deutschland Standeslobby beim BMI derart viel Gehör findet. Der aktuelle IT-Gipfel hat in erschreckender Weise zu erkennen gegeben, dass Datenschutz bei der Bundesregierung derzeit nicht als relevant wahrgenommen wird. Der aktuelle BMI-Entwurf ist ein weiterer Beleg hierfür."

Ob diese unsere Pressemitteilung den Ausschlag gab (die Katze war ja nun aus dem Sack) oder ob wir einfach nur gerade noch rechtzeitig den uns bekannt gewordenen Entwurf vorab veröffentlicht hatten ist eine Frage für ent-

spannte Spekulation. Als Ergebnis gab auf jeden Fall am 23.11.2016 das BMI offiziell den Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) mit Stand vom 23.11.2016 in die Verbändeanhörung[7]. Nach kurzem Querlesen konnten wir auf unserer Seite für die DVD-Pressemitteilungen festhalten, dass zwischen dem geleakten Entwurf vom 11.11.2016 und dem offiziellen Entwurf zur Verbändeanhörung vom 23.11.2016 nur geringfügige Unterschiede bestanden und somit unsere oben abgedruckte Pressemitteilung weiterhin Bestand hatte. Und dann ging das intensive Beschäftigen mit dem Entwurf los. Wir waren ja nun offiziell zur Stellungnahme aufgefordert und in bewährter Manier haben wir in Zusammenarbeit mit den Kolleginnen und Kollegen vom Netzwerk Datenschutzexpertise zusammen an der Stellungnahme gearbeitet und konnten am 04.12.2016 unsere Stellungnahme ans BMI übermitteln und am 05.12.2016 passend dazu eine weitere PM und die Stellungnahme selbst veröffentlichen. Im Folgenden nun die Pressemitteilung[8] und danach die Stellungnahme[9] im Wortlaut:

Qualifizierte Kritik von Datenschützern am BMI-Entwurf für ein neues deutsches Datenschutzrecht

Mit Datum vom 23.11.2016 stellte das Bundesministerium des Innern (BMI) Verbänden einen Referentenentwurf für ein „Datenschutz-Anpassungs-und Umsetzungsgesetz“ zur Stellungnahme zur Verfügung. Mit diesem Entwurf sollen die Europäische Datenschutz-Grundverordnung (DSGVO), die am 25.05.2018 europaweit direkt anwendbar sein wird, umgesetzt und zugleich das nationale Datenschutzrecht modernisiert werden. In ihrer Stellungnahme begrüßt die Deutsche Vereinigung für Datenschutz e.V. (DVD) gemeinsam mit dem Netzwerk Datenschutzexpertise, dass ein solcher Gesetzentwurf vorgelegt wird und dass das bewährte Instrument der betrieblichen/behördlichen Datenschutzbeauftragten beibehalten wird, formuliert aber zu vielen konkreten Regelungsvorschlägen harsche Kritik, u. a.:

- Die bisher geringe Erhöhung der Ausstattung bei den Aufsichtsbehörden der Länder ist völlig ungenügend. Mittelfristig bedarf es in etwa einer Verdreifachung der Ressourcen, insbesondere des Personals.
- Die geplante Regelung zur Videoüberwachung mit der besonderen Hervorhebung öffentlicher Sicherheitsbelange ist europarechts- und verfassungswidrig.
- Die Regelung zur Bestellung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) verstößt hinsichtlich der geforderten Transparenz und den personellen Anforderungen gegen die europarechtlichen Vorgaben.
- Die eingeschränkten Kontroll-und Sanktionsmöglichkeiten der BfDI insbesondere im Sicherheitsbereich untergraben in diesen Bereichen die Effektivität der Datenschutzaufsicht.
- Die Regelungen zur Vertretung der Aufsichtsbehörden der Länder im Europäischen Datenschutzausschuss beeinträchtigen deren Unabhängigkeit.
- Die Einschränkung der Kontrollbefugnisse der Datenschutzaufsicht im Bereich der Berufsgeheimnisse ist inakzeptabel sowie europarechts- und verfassungswidrig.
- Die Möglichkeiten zur Verweigerung von Auskünften an Betroffene sind zu unbestimmt und zu weitgehend.
- Es verbleiben große Regelungsdefizite in Bezug auf die Datenverarbeitung in Beschäftigungsverhältnissen und in der Forschung, in Bezug auf die Beauftragung von IT-Dienstleistern sowie in Bezug auf die Angebote von Herstellern und Anbietern von IT-Produkten.

Werner Hülsmann, stellv. Vorsitzender der DVD: „Es ist erschreckend, mit welcher Ignoranz das Bundesinnenministerium die europäischen Vorgaben zum Datenschutz in Teilen umsetzen möchte. Damit betätigt sich das Ministerium als Bremser. Es verabschiedet sich so von der früheren Funktion Deutschlands, den Datenschutz global und in Europa fortzuentwickeln.“

Thilo Weichert, Mitglied des DVD-Vorstands: „Der Entwurf ist nicht nur politisch nicht akzeptabel, sondern auch ein teilweise klarer Verstoß gegen europäisches Recht und gegen die deutsche Verfassung. Es wäre ein einmaliger Vorgang, wenn das Bundesverfassungsgericht und der Europäische Gerichtshof nicht nur spezifische, sondern grundlegende Regelungen beim Datenschutz aufheben müssten.“ Frank Spaeing, Vorsitzender der DVD: „Dieser Entwurf ist wirtschafts-, fortschritts- und betroffenenfeindlich. Wir hoffen, dass die Kritik der Verbände und der anderen Ministerien dazu führt, dass die bestehenden Defizite behoben werden.“

---

1 DANA 2/2016 zum Download: https://www.datenschutzverein.de/wp-content/uploads/2016/07/DANA_2-2016_RoteLinienRevisited_Web.pdf

2 PM zur Veröffentlichung: https://www.datenschutzverein.de/wp-content/uploads/2016/07/PM-2016-08-01-BDSG-Nachfolgegesetz.pdf

3 https://cdn.netzpolitik.org/wp-upload/2016/09/Referentenentwurf_DSAnpUG_EU.pdf

4 unter anderem https://www.eaid-berlin.de/?p=1309, https://cdn.netzpolitik.org/wp-upload/2016/09/BMJV_Stellungnahme_DSAnpUG_EU.pdf und https://cdn.netzpolitik.org/wp-upload/2016/09/BfDI_Stellungnahme_DSAnpUG_EU.pdf

5 geleakte Version des Gesetzesentwurfs mit Stand vom 11.11.2016: https://www.datenschutzverein.de/wp-content/uploads/2016/11/2016-11-11_DSAnpUG-EU-BDSG-neu_Entwurf-2_Ressortabstimmung.pdf

6 siehe auch https://www.datenschutzverein.de/wp-content/uploads/2016/11/2016-11-22_PM-DVD-BDSG-neu.pdf

7 https://www.datenschutzverein.de/wp-content/uploads/2016/11/161123_BDSG-neu-RefE_-2.-Ressortab-Verbaende-Laender.pdf

8 https://www.datenschutzverein.de/wp-content/uploads/2016/12/2016-12-05-DVD-PM-BSDG-neu.pdf

9 https://www.datenschutzverein.de/wp-content/uploads/2016/12/Stellungnahme_BDSG-neu_DVD_NWDSE_20161204_Web.pdf

Lesen Sie auf den folgenden Seiten die Stellungnahme im Wortlaut.

Stellungnahme der Deutschen Vereinigung für Datenschutz e. V. (DVD) sowie des Netzwerks Datenschutzexpertise

Referentenentwurf des Bundesministeriums des Innern

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

(Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) – Stand 23.11.2016

A Allgemeine Erwägungen

Es wird begrüßt, dass der Bundesgesetzgeber ein Gesetz zur Umsetzung der Europäischen Datenschutzgrundverordnung (EU 2016/679, künftig DSGVO) sowie der der Europäischen Datenschutzrichtlinie für Justiz und Inneres (EU 2016/680, künftig JI-Richtlinie) anstrebt. Nur so kann erreicht werden, dass die Anwender der Regelungen einen rechtssicheren Überblick haben, welche europäischen und nationalen Regelungen Gültigkeit haben, wenn die DSGVO und die JI-Richtlinie im Mai 2018 direkte Wirksamkeit entfalten.

Es sollte darauf geachtet werden, dass nationale Regelungen, denen kein eigenständiger Regelungsgehalt zukommt, europäische Vorgaben **nicht einfach wiederholen**. Vielmehr sollte im Interesse der Klarheit und Rechtssicherheit jeweils auf die direkt anwendbaren Normen verwiesen werden, wenn dadurch nicht die Gesamtverständlichkeit des Normtextes leidet. Bei der Konkretisierung europäischer Normen durch nationale Regelungen auf der Grundlage von sog. Öffnungsklauseln, also der europarechtlichen Zulassung nationaler Rechtsetzung, sollte grundsätzlich ein **Verweis auf die zulassende europäische Norm** erfolgen.

B Ausstattung der Aufsichtsbehörden

In Ihrem Anschreiben wurde darum gebeten, eine Einschätzung abzugeben, welche ggfs. Einsparungen und welcher **Aufwand** sich **für die Länder** aus dem Vollzug des geänderten Datenschutzrechts ergeben. Die neuen Regelungen der DSGVO begründen insbesondere für die Datenschutzaufsicht, also zumeist die Dienststellen der Landesbeauftragten für Datenschutz, Aufgaben insbesondere in folgenden Bereichen:

- Zusammenarbeit mit Verantwortlichen, Auftragsverarbeitern und deren Vertretern (Art. 31 DSGVO),
- Entgegennahme und Bearbeitung der Meldungen von Datenschutzverletzungen (Breach Notification, Art. 33 DSGVO),
- Definition der Kriterien, Entgegennahme, Kommunikation, Prüfung und Bewertung von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 4 – 6 DSGVO) sowie Konsultation bei hohem Risiko (Art. 36 DSGVO),
- Entgegennahme der Meldungen von Datenschutzbeauftragten (Art. 37 Abs. 7 DSGVO) sowie Zusammenarbeit mit diesen (Art. 38 Abs. 1 lit. d, e DSGVO),
- Förderung der Ausarbeitung, Bewertung und Genehmigung von Verhaltensregeln (Art. 40 Abs. 1, 5 DSGVO) sowie die Überwachung und Kommunikation hierzu (Art. 41),
- Förderung und Überprüfung von Zertifizierungen (Art. 42, 43 DSGVO),
- Bewertung des internationalen Datentransfers durch Prüfung und Genehmigung von Vertragsklauseln und anderen Bestimmungen und gegebenenfalls Durchführung von Kohärenzverfahren hierzu sowie internationale Zusammenarbeit (Art. 46 Abs. 3, 4, 47 Abs. 1, 50 DSGVO),
- Wahrnehmung der Aufgaben nach Art. 57 DSGVO (s. o. sowie u. a. Überwachung, Durchsetzung, Information und Beratung für Öffentlichkeit, Verantwortliche u. Auftragsverarbeiter, Bearbeitung von Beschwerden, Zusammenarbeit mit anderen Aufsichtsbehörden, Festlegung von Standardvertragsklauseln und verbindlichen internen Vorschriften),
- Aufbau und Pflege von elektronischen Kommunikationsmitteln (Art. 57 Abs. 2 DSGVO),
- Wahrnehmung der Befugnisse zur Untersuchung, Abhilfe, Genehmigung und Sanktion (Art. 58 Abs. 1-3, 5 DSGVO)
- Wahrnehmung weiterer Befugnisse, z. B. im Bereich der Informationsfreiheit (Art. 58 Abs. 6 DSGVO),
- Erstellen von Jahresberichten (Art. 59 DSGVO),
- Zusammenarbeit mit den Aufsichtsbehörden des Bundes und der Länder (§ 18 BDSG-neu)
- Zusammenarbeit und Durchführung von Kohärenzverfahren (Art. 60-67 DSGVO),
- Zusammenarbeit und Beteiligung (als betroffene Aufsichtsbehörde) im Rahmen der Tätigkeit des Europäischen Datenschutzausschusses (Art. 68 Abs. 4, 70 DSGVO, § 17 BDSG-neu),
- Durchführung von Gerichtsverfahren (Art. 78 DSGVO), Anfechtung von Kommissionsentscheidungen (§ 21 BDSG-neu).

Entsprechende Aufgaben haben die Datenschutzaufsichtsbehörden auch gemäß der **JI-Richtlinie**.

Viele der o. g. Aufgaben gehen **über die bisher bestehenden Aufgaben weit**

hinaus, insbesondere was neue Instrumente, die (internationale) Zusammenarbeit, Genehmigungen und die Durchführung von gerichtlichen Verfahren betrifft.

Das Bundesverfassungsgericht (BVerfG) hat festgestellt, dass insbesondere im für die Betroffenen intransparenten öffentlichen **Sicherheitsbereich** bei den Aufsichtsbehörden regelmäßige Prüfpflichten bestehen, denen viele Aufsichtsbehörden wegen der unzureichenden Ausstattung nicht oder nur unvollständig nachkommen können (BVerfG U. v. 24.04.2013, 1 BvR 1215/07, Rn. 204 ff., 217 – ATDG = NJW 2013, 1517). Es ist unbestritten, dass die Aufsichtsbehörden schon mit ihrer bisherigen Ausstattung den ihnen obliegenden Aufgaben nicht angemessen nachkommen können (Schulzki-Haddouti in Stiftung Datenschutz, Zukunft der informationellen Selbstbestimmung, 2016, S. 111 ff.; diess, Zu kurz gekommen, c´t 17/2015, 76 ff.).

Gemäß Art. 52 Abs. 2 DSGVO stellt jeder Mitgliedstaat sicher, „dass jede Aufsichtsbehörde mit den **personellen, technischen und finanziellen Ressourcen**, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können“.

Die **Mehrausgaben der Länder** beschränken sich nicht auf die Wahl und Bestellung des Stellvertreters des gemeinsamen Vertreters im Europäischen Datenschutzausschuss gem. § 17 BDSG-neu. Insofern ist die Aussage der Gesetzesbegründung „Weiterer neuer Erfüllungsaufwand entsteht für die Verwaltung nicht“ (S. 4) nicht zutreffend, wenn der Gesetzentwurf und die Umsetzung der DSGVO gemeinsam betrachtet werden.

Eine nähere **Bezifferung des Ressourcenbedarfs** bei den Ländern ist im Rahmen der vorliegenden Stellungnahme nicht möglich. Hierfür bedarf es eigenständiger Untersuchungen. Unabhängig hiervon und ungeachtet der teilweise sehr unterschiedlichen Ausstattung der Aufsichtsbehörden in den Ländern ist im Rahmen einer überschlägigen Schätzung zumindest eine Verdreifachung des bisherigen Personals und eine entsprechende Erweiterung der Ressourcen nötig, um die bestehenden und künftigen Aufgaben adäquat erfüllen zu können. Mit der Aufstockung des Personals sollte umgehend begonnen werden um zu verhindern, dass bei kurzfristig nötigen Einstellungen nicht ausreichend qualifiziertes Personal eingestellt wird. Spätestens im Jahr 2020 sollte eine umfassende Erhebung durchgeführt werden, ob und inwieweit die Ausstattung der Aufsichtsbehörden den neuen Anforderungen entspricht.

C Einzelstellungnahme zum Entwurf eines neuen BDSG

Zu § 2 Begriffsbestimmungen

Eine **Wiederholung der Begriffsbestimmungen** aus Art. 4 DSGVO, wie sie in Abs. 2 geplant ist, ist nicht zu empfehlen. Vielmehr sollte auf die DSGVO verwiesen werden. Im Interesse der Rechtsklarheit besteht für den nationalen Gesetzgeber ein sehr weit gehendes Verbot, europäische Regelungen zu wiederholen (Kühling, Martini u. a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 6 ff.; vgl. auch die Gesetzesbegründung S. 68). Für Begriffsbestimmungen im Hinblick auf die JI-Richtlinie (Gesetzesbegründung S. 72) genügt ein Verweis auf die Geltung der Begriffsbestimmungen der DSGVO.

In den in § 2 BDSG-neu enthaltenen Begriffsbestimmungen fehlt eine Zuordnung der in der DSGVO verwendeten Begriffe „Behörde“, „öffentliche Stelle“ und „Unternehmen“ zu den auch im BDSG-neu verwendeten Begriffen „**öffentliche Stelle**“ und „nicht-öffentliche Stellen“. So sind gemäß Art. 4 Ziffer 18 DSGVO auch öffentliche Stellen in öffentlich-rechtlicher Trägerschaft, die am Wettbewerb teilnehmen, als Unternehmen zu betrachten, während nach dem § 2 Abs. 2 Ziff. 3 BDSG-neu nur privatrechtlich organisierte öffentliche Stellen (des Bundes) als nicht-öffentliche Stellen angesehen werden.

Es wird darauf hingewiesen, dass durch das Außerkrafttreten des **bisherigen Bundesdatenschutzgesetzes** (BDSG-alt) gemäß Art. 10 am 25.05.2018 auch die darin enthaltenen Begriffsbestimmungen aufgehoben werden, auf die weiterhin in Kraft befindliche spezifische Regelungen im deutschen Recht Bezug nehmen. Es wird deshalb angeregt, insofern eine Übergangsregelung vorzusehen.

Zu § 3 Verarbeitung durch öffentliche Stellen

Die Regelung ist wegen Art. 6 Abs. 1 lit. e überflüssig, aber auch unschädlich. Es wird empfohlen, eine explizite Bezugnahme zu Art. 6 Abs. 1 lit e DSGVO aufzunehmen.

Zu § 4 Videoüberwachung

Eine materielle Sonderregelung zur Videoüberwachung ist unzulässig, da insofern Art. 6 DSGVO weitgehend abschließend ist (Kühling/Martini u. a. S. 343 ff.; Roßnagel, Europäische Datenschutz-Grundverordnung, 2016, S. 52 f.). Dies gilt auch für den geplanten Abs. 1 Nr. 2, wonach bei Videoüberwachung durch nicht-öffentliche Stellen **Sicherheitsbelange** „in besonderem Maße zu berücksichtigen“ sind. Diese Vorrangregelung bewirkt bei der Interessenabwägung einen Vorrang von Sicherheitsinteressen bei öffentlicher Videoüberwachung, nimmt private Stellen für öffentliche polizeiliche Sicherheitsbelange in Anspruch und verletzt dadurch die Gesetzgebungsbefugnis der Länder, den Verhältnismäßigkeitsgrundsatz sowie spezifische Grundrechte wie z. B. das Versammlungsrecht gemäß Art. 8 GG. Dieses Ergebnis wird verstärkt durch die Regelung in Abs. 3, die bei Erforderlichkeit „zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten“ ohne eine Angemessenheitsprüfung eine Zweckänderung erlaubt. Auf die gesonderte Stellungnahme der DVD und des Netzwerks Datenschutzexpertise vom 06.11.2016 wird verwiesen (https://www.datenschutzverein.de/wp-content/uploads/2016/11/Stellungnahme_Videoueberwachung_06112016.pdf oder https://dvd-ev.de/pm/stvue). Siehe auch Seite 188 in diesem Heft.

Zu § 11 Ernennung und Amtszeit der BfDI

Die § 22 Abs. 1 BDSG-alt übernehmende Regelung des Abs. 1 sieht vor, dass der deutsche Bundestag die Bun-

desbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) „ohne Aussprache auf Vorschlag der Bundesregierung (…) mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder“ wählt. Die Wahl setzt voraus, dass die BfDI „das 35. Lebensjahr vollendet“ hat. In Abs. 1 S. 4 wird geregelt: „Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Insbesondere muss die oder der Bundesbeauftragte über durch einschlägige Berufserfahrung nachgewiesene Kenntnisse des deutschen und europäischen Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Dienst haben.“ Gemäß Abs. 3 ist bei einer Amtszeit von 5 Jahren eine einmalige Wiederwahl zulässig.

Die Beachtung rechtlicher Anforderungen an das Verfahren der Bestellung und die Qualifikation der Datenschutzbeauftragten stand lange Zeit nicht im Fokus öffentlicher Diskussion. Dies hat sich mit dem **Gutachten des Netzwerks Datenschutzexpertise** vom 17.11.2016 geändert, in dem sowohl die rechtlichen Anforderungen wie auch die Praxis kritisch hinterfragt werden. Dabei erweist sich, dass die bisherige Praxis, die mit dem vorliegenden Regelungsvorschlag fortgeschrieben werden soll, gegen Vorgaben des Europarechts und des Verfassungsrechts verstößt (http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_auswahlblfdi5.pdf).

Der Regelungsvorschlag sieht keine öffentliche Ausschreibung der Stelle der BfDI vor und schließt ausdrücklich eine Aussprache über die Wahl aus. Dies steht in Widerspruch zu Art. 53 Abs. 1 DSGVO, wonach das Mitglied der Aufsichtsbehörde „im Wege eines **transparenten Verfahrens** ernannt wird“. Die Transparenzanforderung zielt auf eine öffentliche demokratische Debatte zur Bestellung und die Gewährleistung einer hohen Legitimation und gleicher Chancen der qualifizierten Kandidaten ab. Dies war bisher und würde auch künftig nicht gewährleistet. Die geplante Regelung ist insofern europarechtswidrig.

Art. 33 Abs. 2 Grundgesetz (GG) ist zu beachten, wonach jeder Deutsche „nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amt“ hat.

Das Erfordernis eines **Mindestalters** von 35 Jahren stellt eine nicht gerechtfertigte Altersdiskriminierung dar (Art. 3 Abs. 1 GG, Art. 21 Abs. 1 Europäische Grundrechte-Charta – GRCh). Die abschließenden persönlichen Anforderungen des Art. 53 Abs. 2 DSGVO stellen nicht auf das Alter ab. Der Verweis der Gesetzesbegründung (S. 77) auf Art. 54 Abs. 1 lit. b DSGVO („sonstige Voraussetzungen“) legitimiert keine unsachlichen Anforderungen. Personen unter 35 Jahren können die geforderte Erfahrung und Sachkunde vorweisen. Diese Regelung ist daher verfassungs- und europarechtswidrig.

Das Erfordernis der Befähigung zum **Richteramt oder höheren Dienst** war historisch begründet, als die Datenschutzbeauftragten weitgehend nur für die Kontrolle des öffentlichen Bereichs zuständig waren. Das Erfordernis findet sich nicht in Art. 53 Abs. 2 DSGVO und ist auch keine adäquate Beschreibung der Qualifikation und Sachkunde. Daher sollte auf diese Einschränkung verzichtet werden.

Die Beschränkung auf eine **einmalige Wiederwahl** findet sich nicht in der abschließenden Aufzählung der personellen Anforderungen an das Mitglied der Aufsichtsbehörde in Art. 53 Abs. 2 DSGVO. Amtsinhaber, die zwei Amtsperioden absolviert haben, können regelmäßig die dort geforderte Erfahrung, Qualifikation und Sachkunde vorweisen. In der Praxis hat sich gezeigt, dass durch mehrfach wiedergewählte Datenschutzbeauftragte eine qualifizierte Amtsausübung gewährleistet wird. Angebliche Gründe für eine Beschränkung, etwa Erlahmen der Innovationsbereitschaft, treffen nicht zu. Es gibt keine Wiederwahlverbote in vergleichbaren Positionen. Diese Regelung ist daher verfassungs- und europarechtswidrig.

Zu § 13 Rechte und Pflichten der BfDI

In Abs. 5 S. 2 ist vorgesehen, dass die BfDI keine **Aussagebefugnis als Zeugin** hat, soweit die Aussage laufende oder abgeschlossene Vorgänge betrifft, „die dem Kernbereich exekutiver Eigenverantwortung der Bundesregierung zuzurechnen sind oder sein könnten“. In diesen Fällen muss das „Benehmen mit der Bundesregierung“ hergestellt werden. Was zum Kernbereich exekutiver Eigenverantwortung der Bundesregierung zu zählen ist, ist völlig unklar. Dadurch, dass schon die Möglichkeit eines solchen Betroffenseins dazu führt, dass die Aussagebefugnis von einem Benehmen mit der Bundesregierung abhängig gemacht wird, wird die Unabhängigkeit der BfDI unangemessen beeinträchtigt. Es wird vorgeschlagen, insofern eine Kann-Regelung bzgl. der Aussageverweigerung vorzusehen sowie eine Sollregelung in Bezug auf das Benehmen mit der Bundesregierung.

Zu § 14 Aufgaben der BfDI

Die DSGVO sieht als Aufgabe von Aufsichtsbehörden auch „Datenschutzzertifizierungsmechanismen und von **Datenschutzsiegeln und -prüfzeichen** nach Artikel 42 Absatz 1“ vor. (Art. 57 Abs. 1 lit. n DSGVO). Datenschutz-Zertifizierung gibt es bisher in Deutschland zwar nur auf Länderseite und ist auch künftig als Aufgabe für die BfDI nicht vorgesehen. Dies entspricht nicht den aktuellen technischen und rechtlichen Erfordernissen, die in der DSGVO erkannt und festgelegt werden.

Zu § 16 Befugnisse der BfDI

In Abs. 2 ist vorgesehen, dass außerhalb des Anwendungsbereichs der DSGVO bei der Feststellung von Datenschutzverstößen durch öffentliche Stellen – wie bisher – lediglich als „Sanktion“ eine Beanstandung zulässig ist. Diese Regelung ignoriert die Regelungsintention des neuen europäischen Datenschutzrechts, angesichts der großen Umsetzungsdefizite beim Datenschutz – auch im öffentlichen Bereich – wirksame Sanktionen zu ermöglichen. **Beanstandungen** haben sich insbesondere im Sicherheitsbereich oft als wirkungslos erwiesen, da sie kein rechtliches Instrument sind, mit dem Verantwortliche zu rechtskonformem Vorgehen gebracht werden können. Dies haben zuletzt die Datenschutzverstö-

ße durch den Bundesnachrichtendienst (BND) gezeigt. Mit der Regelung wird gerade im Bereich der JI-Richtlinie sowie der Geheimdienste auf eine effektive Sanktionsform verzichtet. Sollen finanzielle Sanktionen sowie Unterlassungs- und Beseitigungsverfügungen nicht möglich sein, so muss der BfDI zumindest ein Klagerecht vor Gericht gegen rechtswidrige Datenverarbeitung eröffnet werden.

Die Regelung des Abs. 3 S. 1, wonach sich die Befugnisse der BfDI auch auf **Post- und Telekommunikationsgeheimnisse sowie auf Steuergeheimnisse** erstrecken, ist historisch begründet und inzwischen eine Selbstverständlichkeit, welcher es nicht bedarf. Auf sie sollte deshalb verzichtet werden.

Zu § 17 Vertretung im Europäischen Datenschutzausschuss (EDSA)

In Abs. 1 ist vorgesehen, dass die BfDI die gemeinsame Vertretung Deutschlands im Datenschutzausschuss (EDSA) wahrnimmt. Die Stellvertretung soll aus den Leitungen der Landes-Aufsichtsbehörden vom Bundesrat ausgewählt werden. Bei Angelegenheiten, die insbesondere die Länderaufsicht betreffen, soll nach Abs. 2 im EDSA vorrangig die Stellvertretung tätig werden. Diese Regelung ist nicht sachgerecht und beeinträchtigt die Unabhängigkeit der Landesaufsichtsbehörden.

Hauptaufgabe des EDSA wird die Festlegung von Positionen im Bereich des **Datenschutzes im nicht-öffentlichen Bereich** (oder in der Begrifflichkeit der DSGVO: **für Unternehmen)** sein. Insofern hat die BfDI – abgesehen von Post- und Telekommunikationsunternehmen – weder Kompetenzen noch Erfahrungen. Diese liegen vielmehr bei den Landesaufsichtsbehörden.

Durch die **Bestimmung der Stellvertretung** durch den Bundesrat wird dem Bundesrat die Möglichkeit eröffnet, am Willen der Aufsichtsbehörden vorbei unter Anlegung sachfremder Erwägungen für diese deren Vertretung zu benennen. Dies kann zur Folge haben, dass die dadurch in den EDSA eingebrachten Positionen nicht die der unabhängigen Aufsichtsbehörden repräsentieren. Die Regelung ist völlig unangemessen.

Es wird vorgeschlagen, die Bestimmung der Vertretung und der Stellvertretung der deutschen Aufsichtsbehörden diesen selbst zu überlassen. Diese sollten mit qualifizierter Mehrheit ihre **Vertretung im EDSA selbst wählen**. Dieser Vorschlag entspricht der „Kühlungsborner Erklärung" der unabhängigen Datenschutzbehörden der Länder vom 10.11.2016 (https://www.datenschutz.de/kuehlungsborner-erklaerung-der-unabhaengigen-datenschutzbehoerden-der-laender-vom-10-november-2016/).

Zu § 18 Verfahren der Zusammenarbeit der Aufsichtsbehörden

Zur Bestimmung von gemeinsamen Positionen der deutschen Aufsichtsbehörden soll gemäß Abs. 2 zunächst ein **Einigungsverfahren** angestrebt werden. Gelingt eine Einigung nicht, so soll der Vertreter bzw. in Länderangelegenheiten der Stellvertreter ein Bestimmungsrecht haben, „wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen". Wegen der nicht repräsentativen Festlegung der Vertretung (s. o. zu § 17) wird damit in die Unabhängigkeit der Aufsichtsbehörden unangemessen eingegriffen.

Nach Abs. 3 S. 2 soll im Falle, dass eine Einigung unter den deutschen Aufsichtsbehörden nicht möglich ist, der Stellvertreter ein Bestimmungsrecht haben, wenn „die Angelegenheit die Wahrnehmung von Aufgaben betreffen, für welche die Länder alleine das **Recht zur Gesetzgebung** haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betrifft". Die Regelung ist unklar: Das Recht der Gesetzgebung liegt in vielen Fällen des Datenschutzrechtes, insbesondere auch im nicht-öffentlichen Bereich, beim Bund, während die hier in Frage stehende Verwaltungskompetenz bei den Ländern liegt. In der Regelung ist daher der Verweis auf die Gesetzgebungskompetenz zu streichen.

Zu § 22 Verarbeitung besonderer Kategorien personenbezogener Daten

In der Regelung werden wesentliche Inhalte des Art. 9 DSGVO wiederholt, ohne weitere Präzisierungen vorzunehmen. Diese Regelung ist wegen der reinen **Paraphrasierung** ohne eine zusätzliche Regelungsabsicht rechtswidrig (Kühling/Martini u. a., S. 6 ff. m. w. N.). Auf sie sollte verzichtet werden.

In Abs. 2 werden Aussagen gemacht, was **„angemessene und spezifische Maßnahmen** zur Wahrung der Grundrechte und Interessen der betroffenen Personen" gemäß Art. 9 Abs. 1 DSGVO sind. Problematisch ist hierbei, dass auf die „Implementierungskosten" Bezug genommen wird, die in Art. 32 DSGVO bzgl. der informationstechnischen Sicherheit, nicht aber bzgl. der Gestaltung von Verfahren nach Art. 25 DSGVO oder materiell-prozessualen Vorkehrungen relevant sein sollen. Selbstverständlich können solche Kosten bei Angemessenheitsentscheidungen eine Rolle spielen. Deren explizite Erwähnung eröffnet aber die Möglichkeit, spezifische Maßnahmen allein aus Kostengründen zurückzuweisen. Wenig förderlich ist auch der Verweis auf Sensibilisierungs- und Schulungsmaßnahmen (Abs. 2 Satz 2 Nr. 2). Die in Abs. 2 enthaltenen Erwähnungen sind nicht vollständig und weisen erst recht nicht auf eine Priorisierung hin. Die Regelung ist daher nicht geeignet, eine Konkretisierung der europäischen Vorgaben zu bewirken. Daher sollte auf sie verzichtet werden.

Es ist nicht erkennbar, weshalb die Anwendung von Abs. 2 im Fall des Abs. 1 lit. b (**Datenverarbeitung im Gesundheits- und Sozialbereich durch Berufsgeheimnisträger**) ausgeschlossen wird. Zwar werden auch in Art. 9 Abs. 3 DSGVO mit der Regelung zu Berufsgeheimnisträgern die angemessenen spezifischen Sicherungsmaßnahmen erwähnt, doch erfolgt dies systematisch an einem anderen Ort. Es dürfte nicht bestritten werden können, dass solche Maßnahmen auch und gerade erforderlich sind, wenn hochsensible Daten, die Berufsgeheimnissen unterliegen, verarbeitet werden.

Zu § 23 Zweckänderungen

In der Norm werden eine Vielzahl von Zweckänderungen erlaubt, die schon derzeit ihre Erlaubnisgrundlage in der DSGVO finden. Insofern sind sie überflüssig und wegen der **reinen Wiederholung** europäischer Normvorgaben unzulässig.

In Abs. 2 Nr. 1-3 werden Zweckänderungen für **nicht-öffentliche Stellen** erlaubt, für Sicherheitszwecke, zur Geltendmachung rechtlicher Ansprüche und zur Wahrung berechtigter Interessen. Dies entspricht den in Art. 6 Abs. 1 DSGVO vorgegebenen Verarbeitungsbefugnissen, ohne jedoch eine Abwägungsklausel zu enthalten, über welche die schutzwürdigen Betroffeneninteressen zu berücksichtigen sind, so wie dies Art. 6 Abs. 1 lit. f DSGVO explizit fordert. Damit unterschreiten diese Normen in unzulässiger Weise das europäische Schutzniveau. Auf sie kann wegen der bestehenden europäischen rechtlichen Rahmenbedingungen vollständig verzichtet werden.

Die in Abs. 3 enthaltenen Zweckänderungsregelungen für **sensitive Daten** nach Art. 9 DSGVO enthalten auch keine expliziten Abwägungspflichten und paraphrasieren Art. 9 Abs. 2 DSGVO. Auch auf diese allgemeinen Regelungen sollte vollständig verzichtet werden. Bisher besteht im nationalen Recht eine Vielzahl konkretisierender bereichsspezifischer Regelungen, z. B. in den Sozialgesetzbüchern, die ihre Gültigkeit behalten. Diese genügen zur Wahrung der bisherigen – legitimen – Verarbeitungsbefugnisse.

Zu § 24 Verarbeitung von Beschäftigtendaten

Die Wiederauflage des völlig **missglückten § 32 BDSG**-alt ist abzulehnen. Diese Norm führte zu Rechtsunsicherheit, nicht zur Präzisierung von Verarbeitungsbefugnissen und Betroffenenrechten. Zudem darf bezweifelt werden, dass die vorgesehene Regelung den Anforderungen des Art. 88 Abs. 2 DSGVO standhält. Es bedarf vielmehr eines umfassenden Beschäftigtendatenschutzgesetzes, wozu das Netzwerk Datenschutzexpertise die relevanten Rahmenbedingungen in seinem Gutachten vom 08.04.2016 benannt hat (http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_dsgvo_beschds.pdf).

Zu § 25 Zwecke der wissenschaftlichen Forschung

Die geplante Forschungsregelung ist unvollständig und unterschreitet das in der DSGVO vorgeschriebene Niveau. Unvollständig ist Abs. 1 im Hinblick auf sensitive Daten gemäß Art. 9 Abs. 1 DSGVO dadurch, dass eine Konkretisierung von angemessenen Schutzmaßnahmen, wie in Art. 9 Abs. 2 lit. j DSGVO gefordert, unterlassen wird. Art. 89 Abs. 1 DSGVO sieht vor, dass die Datenverarbeitung zu „Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken (…) geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person" zu unterliegen hat. Derartige Schranken enthält der vorgelegte Entwurf nicht. Unvollständig ist die Regelung auch im Hinblick auf die Verarbeitung von Berufsgeheimnissen, z. B. dem Patientengeheimnis unterliegenden Daten, da insofern weiterhin § 203 StGB als Hindernis zur Einbeziehung in Forschungsvorhaben bestehen bleibt. Tatsächlich werden keine ausreichenden und effektiven Schutzmaßnahmen geregelt, sondern lediglich ein Minimalkatalog beliebiger Vorkehrungen. So wird es z. B. unterlassen, ein explizites beschlagnahmesicheres Forschungsgeheimnis festzuschreiben. Unbefriedigend ist die Regelung insgesamt, da sie nicht das Ziel verfolgt, den Wirrwarr unterschiedlicher spezifischer Forschungsklauseln im Bundes- und im Landesrecht zu vereinheitlichen und zu modernisieren. Zur Sicherung des Datenschutzes in der Forschung und einer damit verbundenen Stärkung des Forschungsstandortes Deutschland bedarf es eines umfassenden **Forschungsgesetzes**, das, um auch die Regelungsebene der Länder mit einzuschließen, als Bund-Länder-Staatsvertrag erlassen werden sollte.

Zu § 26 Berufsgeheimnisse

Die Regelung beschreibt nur völlig unzureichend, welche Daten mit ihr erfasst werden sollen und ist deshalb **zu unbestimmt**: Die Formulierung „Daten, die nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, einer Geheimhaltungspflicht unterliegen" könnte auf jede Form eines spezifischen Geheimnisses angewendet werden, nicht nur auf Berufsgeheimnisse nach § 203 Abs. 1, (2a,) 3 StGB, § 53, 54 StPO, sondern auch auf das Sozialgeheimnis nach § 35 SGB I, ja sogar auf weitgehend unreguliert bleibende Betriebs- und Geschäftsgeheimnisse. In der Literatur wird diese Regelung – fälschlich – gar auf Amtsgeheimnisse wie z. B. das Statistik- oder das Meldegeheimnis erstreckt (Paal/Pauly, Datenschutz-Grundverordnung, 2016, Art. 90 Rn. 6). Es bedarf vielmehr einer rechtssicheren Verweisung auf einen engen Kranz aus besonderen Gründen gesondert zu behandelnder Daten.

Gemäß den Absätzen 1 und 2 werden das Informationsrecht nach Art. 14 DSGVO und das **Auskunftsrecht** nach Art. 15 DSGVO eingeschränkt, „wenn die Daten geheim gehalten werden müssen und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss". Die Unbestimmtheit der erfassten Daten erstreckt sich auf diese Beschränkung informationeller Selbstbestimmung generell und des Auskunftsanspruchs als „Magna Charta des Datenschutzes" (s. u. zu § 32). Damit wird die grundlegende Garantie des Auskunftsanspruchs in Art. 8 Abs. 2 S. 2 GRCh verletzt. Diese Unbestimmtheit wird erweitert durch eine völlig offene Abwägungsnorm, die weder für Anwender noch für Betroffene einschätz- und berechenbar ist. Die Einschränkung des Auskunftsanspruchs muss sich auf spezifische Fallgestaltungen beschränken, die notwendig und verhältnismäßig sind. Die vorliegende Regelung genügt diesen Anforderungen nicht und ist europarechts- und verfassungswidrig.

In Abs. 3 werden die in Abs. 1 beschriebenen Daten pauschal einer stark **beschnittenen Datenschutzkontrolle** durch die zuständige Aufsicht unterworfen. Kontrollbefugnisse sollen nur zwecks Überprüfung der Einhaltung des Art. 25 DSGVO bestehen. Art. 25 DSGVO bezieht sich auf die Technikgestaltung und datenschutzfreundliche Voreinstellungen, also auf technische und organisatorische Maßnahmen. Dabei bleibt der vorgesehene Kontrollumfang unklar, da er Art. 32, d. h. die technische Sicherheit der Verarbeitung, nicht umfasst. Umfasst sein sollen offensichtlich auch nicht Fragen der materiellen Zulässigkeit der Verarbeitung. Bisher ist es unbestritten, dass zu den in die Kontrolle einbezogenen Daten auch Berufsgeheimnisse gehören. Bisher gehört

die Kontrolle der Wahrung des Patienten- und den Sozialgeheimnisses zu den Schwerpunkten der aufsichtsbehördlichen Tätigkeit. Diese würde vollständig ausgeschlossen, selbst dann, wenn die Kontrolle auf Beschwerde von Betroffenen erfolgen würde. Im ärztlichen und psychologischen Bereich wurde die Datenschutzkontrolle bisher auch von den geprüften Stellen nicht in Frage gestellt. Sie ist vielmehr oft ein Instrument, um das Vertrauen in die jeweiligen Stellen zu erhöhen.

Durch die vorgesehene weitgehende Ausnahme von der Datenschutzkontrolle wird das von der DSGVO verfolgte Ziel einer weitgehenden **Harmonisierung** verfehlt. Sie hat auch zur Folge, dass vom Europäischen Datenschutzausschuss gemäß Art. 70 DSGVO erarbeitete Leitlinien, Empfehlungen und bewährte Verfahren nur begrenzt ein- und umgesetzt werden können.

Die Begründung (S. 93) verweist auf die bundesverfassungsgerichtliche Rechtsprechung, wonach das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet werden darf (BVerfG U. v. 12.04.2005, NJW 2005, S. 1917). Dies schließt aber eine externe Kontrolle der Rechtmäßigkeit des Berufsgeheimnisträgers nicht aus. Es genügt, dass Abs. 2 S. 2 die Geheimhaltungspflicht auf die Aufsichtsbehörde verlängert und ein Beweisverwertungsverbot im Strafverfahren schafft. Politisch angegriffen wird die Kontrollbefugnis der Datenschutzaufsicht im nicht-öffentlichen Bereich ausschließlich durch Anwaltsorganisationen. Praktische Probleme sind in diesem Bereich aber in der 40-jährigen Aufsichtsgeschichte nur in wenigen Einzelfällen aufgetreten, die durch eine Berücksichtigung des **Mandantengeheimnisses** bei der Datenschutzkontrolle aufgelöst werden konnten. Der Anwaltschaft geht es darum, sich der unabhängigen Datenschutzkontrolle nicht zum Schutz der Mandanten und des Mandantengeheimnisses zu entziehen, sondern zur Freistellung von Kontrolle generell. Es ist unbestreitbar, dass auch Anwälte dem Datenschutzrecht unterliegen und unterliegen müssen (ausführlich dazu Weichert NJW 2009, 550 ff.; Weichert in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2016, § 38 Rn. 11 m. w. N.).

Es ist nicht erkennbar, wie eine Datenschutzkontrolle durchgeführt werden soll, die sich auf Art. 25 DSGVO beschränkt, da mit einer Kontrolle von Art. 25 DSGVO oft zwangsläufig die Kenntnisnahme von Berufsgeheimnissen verbunden ist. Eine **Trennung auf Kontrollebene** zwischen technischem und materiellem Datenschutz ist zumeist nicht möglich.

Art. 90 DSGVO erlaubt nur Einschränkungen der Datenschutzkontrolle, die „**notwendig und verhältnismäßig**" sind. Hierzu gibt es weder im Gesetzestext noch in der Begründung Ausführungen. Vielmehr ist die geplante Einschränkung in ihrem Umfang sachlich nicht begründet und nicht zu begründen. Datenschutzverstöße durch Berufsgeheimnisträger werden dadurch vollständig kontroll- und damit auch sanktionsfrei gestellt, so dass die Schutzfunktion unabhängiger Datenschutzkontrolle, die in Art. 8 Abs. 3 GRCh ausdrücklich festgeschrieben ist, verloren geht. Die Regelung ist daher verfassungs- und europarechtswidrig. Auf sie kann und sollte ersatzlos verzichtet werden.

Zu § 27 Datenübermittlung an Auskunfteien

Die Übernahme dieser Regelung aus dem BDSG-alt ist in Bezug auf den Regelungsinhalt grundsätzlich zu begrüßen. Es ist aber in Frage zu stellen, ob „die Ermittlung der Kreditwürdigkeit und die Erteilung von Bonitätsauskünften" ein „wichtiges Ziel des allgemeinen öffentlichen Interesses" der Bundesrepublik Deutschland darstellt und damit, ob die Öffnungsklausel aus Art. 6 Abs. 4 i. V. m. Art. 23 Abs. 1 DSGVO greift.

Zu § 28 Scoring

Mit der Regelung soll der bisherige § 28b BDSG-alt fortgelten. Es ist fraglich, inwieweit dies durch die abschließenden Regelungen des Art. 6 Abs. 1 DSGVO ausgeschlossen ist. Wenn dies verneint wird, sind gemäß Art. 22 Abs. 2 lit. b DSGVO in jedem Fall angemessene **Maßnahmen zur Wahrung der Rechte und Freiheiten** und berechtigten Interessen der Betroffenen zu gewährleisten (Roßnagel, S. 141; Kühling/Martini u. a., S. 440 ff.). Angesichts der in Deutschland gesammelten Erkenntnisse zum Scoring ist fraglich, ob dies der Fall ist. So zeigt sich, dass bei der Eingrenzung der zulässigen Datenarten und Quellen, hinsichtlich der Einbeziehung von Sekundärdaten, der Kontrolle der Verfahren und der geforderten Relevanz und Prognosegüte große Regelungsdefizite bestehen und neue Formen des Scoring, die über die klassische Bonitätsbewertung hinausgehen, nicht hinreichend abgedeckt sind (ausführlich Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014, http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Scoring-Studie.pdf?__blob=publicationFile&v=3).

Zu § 30 Informationspflichten bei der Erhebung bei Betroffenen

Nach Abs. 1 Nr. 2 rechtfertigt schon ein „**unverhältnismäßiger Aufwand**" den Verzicht auf Informationen nach Art. 13 DSGVO zur Verarbeitung bei einer Betroffenenerhebung. Diese äußerst unbestimmte Norm ermöglicht es Verantwortlichen, ohne weiteren Rechtfertigungsbedarf keine Betroffeneninformationen bereitzustellen. Die Schwelle zur Rechtfertigung fehlender Transparenz ist zu erhöhen.

Entgegen der Regelung in Abs. 3 Satz 2 ist sofort mit der Aktivierung von Kameras über eine **Videoüberwachung** zu informieren und nicht erst zum frühestmöglichen Zeitpunkt. Die Regelung bietet Verantwortlichen Schlupflöcher, den Zeitpunkt nach hinten zu verlagern. Hier muss ein Verringern des bisherigen Niveaus (§ 6a Abs. 2 BDSG-alt) vermieden werden.

Zu § 31 Informationspflichten bei Dritterhebung

Gemäß Abs. 1 Nr. 1 lit. a genügt schon eine **Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben** einer öffentlichen Stelle, um auf eine Information der Betroffenen nach Art. 14 DSGVO zu verzichten. Angemessen ist nur eine höhere Schwelle, etwa die Beeinträchtigung einer zulässigen Aufgabenerfüllung.

Abs. 1 Nr. 2 lit. a legitimiert die Nichtinformation der Betroffenen, wenn eine

erhebliche **Gefährdung der Geschäftszwecke** des Verantwortlichen angenommen wird. Dies eröffnet ein hohes Missbrauchspotenzial, da die Geschäftszwecke einseitig durch den Verantwortlichen definiert werden. Es bedarf insofern ergänzender Schutzmaßnahmen. Die in Abs. 2 genannten Vorkehrungen, die zu „geeigneten Maßnahmen zur Information für die Öffentlichkeit" verpflichten, genügen zur Verhinderung von Missbrauch der Transparenzausnahme nicht.

Zu § 32 Einschränkung des Auskunftsanspruchs

Abs. 1 Nr. 1 rechtfertigt die Auskunftsverweigerung bei Vorliegen eines Grundes zum Verzicht auf Informationen nach den §§ 30, 31. Dies hat zur Folge, dass schon mit der **Gefährdung der Aufgabenerfüllung** oder der erheblichen Gefährdung der Geschäftszwecke die Auskunftsverweigerung begründet werden kann. Angesichts des hohen Rangs des grundrechtlich in Art. 8 Abs. 2 S. 2 GRCh garantierten Anspruchs auf Auskunft – der Magna Charta des Datenschutzes (z. B. Mallmann in Simitis, BDSG, 8. Aufl. 2014, § 19 Rn. 1) – ist dies unverhältnismäßig.

Dies gilt erst recht für die Möglichkeit für nicht-öffentliche Stellen nach Abs. 2, die Auskunft unter Verweis auf die Wahrung von **Geschäftsgeheimnissen** zu verweigern. Individuelle Daten eines Betroffenen können nicht als Geheimnisse diesem gegenüber anerkannt werden (ULD/GP Forschungsgruppe, Scoring-Gutachten, S. 44 ff. gegen BGH NJW 2014, 341). Die Ausnahme von der Auskunft ist ersatzlos zu streichen.

Zu § 33 Einschränkung der Löschungsverpflichtung

Abs. 1 sieht vor, dass keine Löschpflicht besteht, „wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit **unverhältnismäßigem Aufwand** möglich ist". Diese Regelung steht im Widerspruch zu Art. 25, 32 DSGVO zu den technisch-organisatorischen Maßnahmen, wozu auch die Intervenierbarkeit von Daten gehört, die bei der Gestaltung der Systeme beachtet werden muss. Automatisierte Verfahren, die in der Vergangenheit nicht in der Lage waren, spezifische Löschungen vorzunehmen, wurden inzwischen überarbeitet. Die Norm würde dazu einladen, Verfahren zu etablieren, mit denen mangels Löschbarkeit der Daten auf obligatorische Datenlöschungen verzichtet werden könnte.

Zu § 34 Einschränkung des Widerspruchsrechts

Nach der Regelung besteht kein Recht auf Widerspruch nach Art. 21 Abs. 1 DSGVO, wenn die Verarbeitung erforderlich und der Widerspruch „die Verwirklichung des Zwecks der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde". Die Verarbeitung der Daten soll nur für Zwecke des § 22 Abs. 1 (Erlaubnisnorm für sensitive Daten) zulässig sein. Eine Zweckänderung soll nur entsprechend Art. 21 Abs. 1 S. 2 DSGVO zulässig sein. Dieser Vorschlag bringt das Recht, Widerspruch einzulegen und das Recht, auf der Grundlage eines Widerspruchs eine Veränderung bei der Datenverarbeitung zu bewirken, durcheinander. Ein Widerspruch ist für sich nicht in der Lage, einen Verarbeitungszweck ernsthaft zu beeinträchtigen, sondern lediglich die sich evtl. daraus ergebende Einschränkung der Verarbeitung. Die Bezugnahme auf sensitive Daten erschließt sich nicht. Ebenso wenig erschließt sich der Verweis auf Art. 21 Abs. 1 S. 2 DSGVO. Die Regelung ist überflüssig und sollte gestrichen werden.

Zu § 36 Datenschutzbeauftragte nicht-öffentlicher Stellen

Es ist zu begrüßen, dass die **bewährten Regelungen aus dem BDSG-alt** in das BDSG-neu übernommen werden. Immer noch sehr viele Unternehmensleitungen sind der Ansicht, dass sie sich nicht um die Umsetzung des Datenschutzes kümmern müssten, solange sie keinen Datenschutzbeauftragten zu bestellen haben. Diese Einstellung kann sich durch die deutlich gestiegenen Höchstgrenzen für Bußgelder im Lauf der Zeit wandeln. Aber durch die Beibehaltung der bisherigen Regelungen zur Bestellpflicht von Datenschutzbeauftragten wird eine präventive Umsetzung des Datenschutzes – die aus Betroffenensicht unbedingt erforderlich ist – gefördert.

Zu § 37 Akkreditierung von Zertifizierungsstellen

Die nationale Umsetzungsnorm zu den Art. 42, 43 DSGVO zur datenschutzrechtlichen Zertifizierung und zur Erteilung von Datenschutzgütesiegeln und -prüfzeichen beschränkt sich darauf, die zuständigen Aufsichtsbehörden in Bund und Ländern zu verpflichten, sich gegenseitig und die Deutsche Akkreditierungsstelle über die Erteilung, Versagung und den „Widerruf einer Akkreditierung" zu unterrichten. Diese äußerst schlanke Regelung lässt praktisch alles hinsichtlich der Akkreditierung von Prüfstellen und der von diesen vorzunehmenden Zertifizierungen im **Unklaren**. Dies veranlasst die Aufsichtsbehörden und die Deutsche Akkreditierungsstelle, alles Wesentliche in eigener Verantwortung zu regeln. Dies ist äußerst unbefriedigend.

Zu § 38 Aufsichtsbehörden im nicht-öffentlichen Bereich

Der Entwurf lässt offen, ob P**ost- und Telekommunikationsunternehmen** – wie bisher (§ 115 Abs. 4 TKG, § 42 Abs. 3 PostG) – von der BfDI oder von den Aufsichtsbehörden der Länder kontrolliert werden sollen.

Zu § 40 Verhängung von Geldbußen

Abs. 3 sieht vor, dass gegen Behörden und **öffentliche Stellen des Bundes** keine Geldbußen verhängt werden, soweit diese nicht wettbewerblich tätig sind. Mit der Regelung, die sich auf die Öffnungsklausel des Art. 83 Abs. 7 DSGVO beruft, werden öffentliche Stellen von Bußgeldverfahren vollständig freigestellt. Dies entspricht nicht den Intention der DSGVO und dem Ziel, die bestehenden Vollzugsdefizite durch verbesserte Sanktionen – im öffentlichen wie im nicht-öffentlichen Bereich – abzubauen.

Zu § 42 Strafantragserfordernis

Zur Strafverfolgung von Verstößen nach § 41 bedarf es eines Antrags. Antragsberechtigt sollen sein „die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde". Damit sollen strafbare

Datenschutzverstöße weiterhin kein Offizial-, sondern ein **Antragsdelikt** sein, was der gesellschaftlichen Bedeutung vieler Datenschutzdelikte nicht gerecht wird (Schulzki-Haddouti, Papiertiger, c´t 10/2016, 162 ff.).

Zu Teil 3 (§§ 43-79) Verarbeitung nach der JI-Richtlinie

Zu den Regelungsvorschläge der §§ 43 bis 79 wird aktuell keine Stellung genommen. Eine spätere Bewertung bleibt vorbehalten.

D Weitere gesetzliche Änderungen

Zu Artikel 2 Änderung des Bundesverfassungsschutzgesetzes

In § 26a Abs. 2 ist vorgesehen, die Datenschutzkontrolle der BfDI auszuschließen, „soweit die Einhaltung von Vorschriften der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegt". In der Vergangenheit hat sich gezeigt, dass die Datenschutzkontrolle der bundesdeutschen Geheimdienste unzureichend ist. Ein Grund hierfür liegt darin, dass die G-10-Kommission und die Kontrolle durch die BfDI sich gegenseitig ausschließen, obwohl in tatsächlicher wie auch in rechtlicher Hinsicht Überschneidungen bestehen. Die **Kontrolle durch die G-10-Kommission** und die BfDI unterscheiden sich sowohl hinsichtlich der Methode wie auch der Fragestellung. Es ist daher gerechtfertigt, sich überschneidende Kontrollen zuzulassen. Hierdurch wird auch vermieden, dass z. B. durch Zuordnungsprobleme kontrollfreie Räume entstehen. Entgegen der Gesetzesbegründung (S. 120) ist die Regelung nicht geeignet, die bisher aufgetretenen Kontrolllücken zu beseitigen. Es ist nicht erkennbar, weshalb, wie in der Begründung aufgeführt, zwischen der G-10-Kommission und der BfDI konträre Ergebnisse entstehen können sollen. Selbst wenn dies der Fall wäre, bestünde insofern kein „Risiko", sondern allenfalls die Chance einer zweiten Meinung, zumal weder der BfDI noch der G-10-Kommission exekutive Durchgriffsrechte zugestanden werden.

In § 27 Abs. 1 ist vorgesehen, dass § 16 Abs. 1 des neuen BDSG nicht gelten soll, welcher der BfDI bei Feststellung von Datenschutzverstößen Untersuchungs- und Abhilfebefugnisse gemäß der DSGVO zugesteht, nachdem eine umfassende Anhörung stattgefunden hat. Es ist nicht erkennbar, weshalb diese Regelung, die die Abstellung von Datenschutzverstößen sicherstellen soll, für nicht anwendbar erklärt wird.

Zu Artikel 7 - Änderung des aktuellen Bundesdatenschutzgesetzes

§ 42b - Antrag der Aufsichtsbehörde auf gerichtliche Überprüfung von Angemessenheitsbeschlüssen der EU-Kommission

Es ist zu begrüßen, dass diese Regelung als eigenständige Änderung in das BDSG-alt eingefügt werden soll (siehe Art. 10 - Inkrafttreten/Außerkrafttreten) und am Tag nach der Verkündung dieses Gesetzes – und nicht erst am 25.05.2018 – in Kraft treten soll.

E Weiterer dringender Änderungsbedarf beim Datenschutzrecht

Der Entwurf behandelt einige Bereiche des Datenschutzes nicht, die dringend einer Regelung bedürfen.

Abgesehen von den schon genannten Themen des Beschäftigtendatenschutzes sowie des Datenschutzes im Bereich der Forschung gilt dies insbesondere für eine Regulierung der Auftragsdatenverarbeitung von Berufsgeheimnissen unterliegenden Verantwortlichen. In seiner Stellungnahme „Datenschutzrechtlicher Handlungsbedarf 2016 für die deutsche Politik nach Verabschiedung der EU-DSGVO" vom 09.05.2016 hat das Netzwerk Datenschutzexpertise darauf hingewiesen, dass IT-Dienstleister, die z. B. Anwalts- oder Arztpraxissysteme administrieren oder hochkomplexe IT-Systeme in Krankenhäusern oder medizinischen Laboren verwalten, nicht den in der StPO gesicherten Vertraulichkeitsschutz genießen und nicht der straf- und standesrechtlichen Schweigepflicht unterliegen, weshalb Berufsgeheimnisträger diesem Personenkreis nach dem derzeit geltenden Recht keinen Zugang zu Patienten- oder Klientendaten gewähren dürfen (http://www.netzwerk-datenschutzexpertise.de/sites/default/files/empf_2016_nat_regelungsbedarf.pdf). Dies beeinträchtigt die Aufgabenwahrnehmung der besonders geschützten Berufsgruppen und letztlich die Rechtssicherheit aller Beteiligten. Dem kann durch eine Erweiterung der Geheimhaltungspflicht und durch eine Offenbarungsbefugnis abgeholfen werden.

In der DSGVO und in der Folge auch im nationalen Umsetzungsgesetz besteht zudem ein großes datenschutzrechtliches Defizit darin, dass als Adressaten der Normen lediglich Verantwortliche und Auftragsverarbeiter benannt werden, nicht aber Hersteller bzw. **Anbieter von IT-Produkten** (Hard- und Software), mit denen personenbezogene Daten verarbeitet werden. Tatsächlich beruhen viele Gefährdungen und Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung darauf, dass Verantwortliche oder Auftragsverarbeiter IT-Produkte einsetzen, die nicht den Anforderungen der DSGVO (z. B. der Art. 25, 32) genügen bzw. genügen können. In Ermangelung einer hinreichenden Kontrolle oder von technischen Einflussmöglichkeiten ist dies Verantwortlichen bzw. Auftragsverarbeitern oft nicht bewusst oder für diese nicht korrigierbar. Vorgegebene Verarbeitungsvorgänge, etwa in Form von Online-Formularen oder voreingestellten Datenweiterleitungen, sind oft weder hinreichend dokumentiert noch durch die (formalrechtlich verantwortlichen) Nutzenden beeinflussbar. Die ungenügende Umsetzung von Privacy by Default und Privacy by Design (vgl. auch Art. 25 DS-GVO) oder generell unterlassene Maßnahmen zur Erhöhung der IT-Sicherheit durch die Hersteller führen oft dazu, dass nötige technisch-organisatorische Maßnahmen unterbleiben oder materiell-rechtliche Verstöße vorgegeben werden.

Ein modernes Datenschutzgesetz muss daher – ähnlich wie eine Adressierung von Straßenverkehrsvorschriften an die Kfz-Hersteller – auch die Hersteller und Anbieter von IT-Produkten, die der personenbezogenen Datenverarbeitung dienen, einbeziehen. Dies kann in der Form erfolgen, dass diesen z. B. bestimmte **verpflichtende Datenschutzstandards** präventiv wirkend vorgegeben werden oder dadurch, dass diesen im Fall datenschutzwidriger Produkte Haftungsrisiken auferlegt werden. Die bisher vorgesehenen freiwilligen Zertifizierungen, die auf eine Selbstregulierung des Marktes setzen, genügen nicht, um die systematische Verbreitung von Datenschutzverstößen einzudämmen.

Pressemitteilung und Stellungnahme der Deutschen Vereinigung für Datenschutz e. V. (DVD) sowie des Netzwerks Datenschutzexpertise zum Videoüberwachungsverbesserungsgesetz

Keine sinnlose Videoüberwachung

Pressemitteilung vom 07.11.2016

Die Deutsche Vereinigung für Datenschutz (DVD) und das Netzwerk Datenschutzexpertise lehnen den Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes ab.

Beide Organisationen bemängeln, dass die geplante Änderung des Bundesdatenschutzgesetzes einen unverhältnismäßigen Eingriff in die Persönlichkeitsrechte Betroffener vorsieht, die privaten Betreiber von Videoanlagen zu polizeilichen Hilfsdiensten heranziehen will und eine unangemessene Beeinflussung der aufsichtsbehördlichen Bewertung von Videoüberwachungsanlagen beabsichtigt.

Dazu Werner Hülsmann, stellvertretender Vorsitzender der DVD: „Die vom BMI durch die geplante Gesetzesänderung ausdrücklich erwartete ‚steigende Anzahl von Videokameras‘ stellt einen erheblichen Eingriff in das Versammlungs- und Demonstrationsrecht dar. Bereits jetzt zeigt die Praxis, dass die zur Wahrung des Versammlungsrechts erforderliche Abschaltung der Kameras während der Versammlungen und Demonstrationen nur unzureichend erfolgt. Zudem ist es für potentielle TeilnehmerInnen nicht erkennbar, ob die Kameras aktiv sind oder nicht.“

Ergänzend Frank Spaeing, Vorsitzender der DVD: „Das Gesetz zielt explizit darauf ab, die unabhängige Tätigkeit der Datenschutzbehörden zu beeinflussen. Es steht dem Gesetzgeber nicht an, die verfassungsrechtlich gesicherte unabhängige Aufgabenwahrnehmung der Datenschutzaufsichtsbehörden bei der grundrechtlichen Abwägung zu beeinflussen.“

Abschließend Thilo Weichert, Vorstandsmitglied der DVD und Autor der Stellungnahme: „Der Eindruck ist nicht von der Hand zu weisen, dass mit dem Entwurf neben dem Versuch, bei der Videoüberwachung Datenschutzbelange hinter Sicherheitsinteressen massiv zurückzudrängen, im Hinblick auf die Bundestagswahl im Herbst 2017 sicherheitspolitische Symbolpolitik betrieben wird.“

Stellungnahme der Deutschen Vereinigung für Datenschutz e. V. (DVD) und des Netzwerks Datenschutzexpertise zum Referentenentwurf des Bundesministeriums des Innern (Stand 02.11.2016)

Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz)

Gemäß dem Gesetzentwurf ist vorgesehen, in § 6b Abs. 1 BDSG folgenden Satz 2 anzufügen:

„Bei öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Einrichtungen und Fahrzeugen des öffentlichen Personenverkehrs ist der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als wichtiges öffentliches Interesse bei der Abwägungsentscheidung nach Satz 1 Nummer 3 in besonderem Maße zu berücksichtigen.“

Außerdem soll nach § 6b Abs. 3 S. 1 BDSG folgender Satz eingefügt werden:

„Absatz 1 Satz 2 gilt entsprechend.“

Die DVD und das Netzwerk Datenschutzexpertise lehnen die geplante Gesetzesänderung ab.

Begründung

Der Intention, Anschläge von Terroristen und Straftätern auf hochfrequentierten öffentlich zugänglichen Anlagen und Plätzen zu erfassen und evtl. „frühestmöglich zu verhindern“, ist uneingeschränkt zuzustimmen. Die geplante Gesetzesänderung ist hierfür aber weder geeignet noch notwendig. Die Gesetzesänderung würde aber voraussichtlich dazu führen, dass an öffentlichen Orten in unverhältnismäßiger Weise Videoüberwachung ausgeweitet wird und dadurch eine massive unverhältnismäßige Einschränkung des Rechts auf informationelle Selbstbestimmung erfolgt.

Keine Gesetzgebungskompetenz

Zudem besteht für die geplante Regelung, deren Hauptziel die Gefahrenabwehr ist, keine Gesetzgebungskompetenz; diese liegt bei den Ländern.

Die geplante Regelung richtet sich nicht an Gefahrenabwehrbehörden, sondern generell an öffentliche Bundesstellen sowie an nicht-öffentliche Stellen. Die Aufgabe der Gefahrenabwehr, die mit dem Entwurf verfolgt wird, insbesondere die Verhinderung von (terroristischen) Anschlägen, gehört nicht zu den Aufgaben der von § 6b BDSG erfassten Stellen, sondern zu den Aufgaben der Polizei, deren Befugnisse bereichsspezifisch im Polizeirecht und nicht im BDSG geregelt sind. Die Gefahrenabwehr obliegt vorrangig den Landespolizeien. Die **Gesetzgebungskompetenz** hierfür liegt bei den Bundesländern (Art. 70 GG). Eine Rechtfertigung der Gesetzgebung durch den Bund über Annexe (z. B. Strafverfahren, Art. 74 Nr. 1 GG; Recht der Wirtschaft, Art. 74 Nr. 11 GG; Straßenverkehr Art. 74 Nr. 22 GG) ist nicht möglich, da der Schwerpunkt der Regelung eindeutig und ausdrücklich in der Gefahrenabwehr liegt. Die

Zuständigkeit nach Art. 73 Abs. 1 Nr. 9a GG für die „die Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht“, ist nicht einschlägig, da sich die Videoüberwachung nicht auf konkrete terroristische Gefahren beschränkt, sondern generell und anlasslos den öffentlichen Raum erfasst. Die Berufung auf das „Recht der Wirtschaft“ im Entwurf geht fehl, da vorrangig Zwecke der Gefahrenabwehr und ausschließlich staatliche Sicherheitszwecke verfolgt werden und – anders als im Entwurf (dort S. 4) behauptet – keine Rechtszersplitterung droht.

Übermäßiger Eingriff in Persönlichkeitsrechte

Das Bundesverfassungsgericht (BVerfG) hat darauf hingewiesen, dass die Videoüberwachung eines öffentlichen Platzes „in das allgemeine Persönlichkeitsrecht potenzieller Besucher des Platzes in seiner Ausprägung als Recht der informationellen Selbstbestimmung“ eingreift (BVerfG B. v. 23.02.2007 – 1 BvR 2368/06, NVwZ2007, 688 ff.). Es hat u. a. Folgendes ausgeführt: „Videoüberwachung ist ein **intensiver Eingriff**. Sie beeinträchtigt alle, die den betroffenen Raum betreten. Sie dient dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken. Das Gewicht dieser Maßnahme wird dadurch erhöht, dass infolge der Aufzeichnung das gewonnene Bildmaterial in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden kann. … Die Videoüberwachung und die Aufzeichnung des gewonnenen Bildmaterials erfassen daher – wie bei solchen Maßnahmen stets – überwiegend Personen, die selbst keinen Anlass schaffen, dessentwegen die Überwachung vorgenommen wird“ (Rn. 52 des Beschlusses).

„Es ist nicht ausgeschlossen, dass eine Videoüberwachung öffentlicher Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials auf der Grundlage einer **hinreichend bestimmten und normenklaren Ermächtigungsgrundlage** materiell verfassungsgemäß sein kann, wenn für sie ein hinreichender Anlass besteht und Überwachung sowie Aufzeichnung insbesondere in räumlicher und zeitlicher Hinsicht und im Hinblick auf die Möglichkeit der Auswertung der Daten das Übermaßverbot wahren“ (Rn. 56 des Beschlusses).

Der Entwurf weist zu Recht darauf hin, dass nach der bestehenden Regelung des § 6b BDSG, dessen Verfassungsgemäßheit nicht angezweifelt wird, „schon heute Sicherheitsbedürfnisse einbezogen werden“. Die Änderung sei nur deshalb nötig, weil „sich eine restriktive Aufsichtspraxis beim Einsatz optisch-elektronischer Sicherheitstechnologien herausgebildet“ habe. Es sei deshalb „notwendig, eindeutigere Vorgaben hinsichtlich der Abwägungsentscheidung zu machen und der Sicherheit und dem **Schutz der Bevölkerung** ein größeres Gewicht beizumessen, wenn es um die Zulässigkeit der Videoüberwachung bei solch hochfrequentierten Anlagen geht“ (S. 1, 4 des Entwurfes). Diese Aussage trifft nicht zu. Durch die geplante Änderung werden keine neuen Abwägungsaspekte eingeführt; der Schutz der Bevölkerung ist schon immer ein zentraler Abwägungsaspekt bei der Beurteilung durch die Betreiber, die Aufsichtsbehörden und die Rechtsprechung. Gerichtliche Überprüfungen der bisherigen Aufsichtspraxis haben insofern bisher keine wesentlichen Änderungsbedarfe ergeben (vgl. z. B. VG Hannover U. 14.07.2011, - 10 A 5452/10, DANA 2011, 131 ff., DÖV 2011, 860).

Unangemessene Beeinflussung der Aufsichtsbehörden

Das Gesetz zielt explizit darauf ab, die **unabhängige Tätigkeit der Datenschutzbehörden** zu beeinflussen. Deren Unabhängigkeit wird in Art. 8 Abs. 3 Grundrechte-Charta (GRCh) sowie durch die deutsche und europäische Verfassungsrechtsprechung bestätigt (BVerfG NJW 1984, 422 f. – Volkszählung; BVerfG NJW 2013, 1499 – Antiterrordatei, Rn. 214 ff.; weitere Nachweise bei Weichert in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2016, § 23 Rn. 2, § 38 Rn. 6). Es steht dem Gesetzgeber nicht an, die verfassungsrechtlich gesicherte unabhängige Aufgabenwahrnehmung der Datenschutzaufsichtsbehörden bei der grundrechtlichen Abwägung zu beeinflussen.

Die der Entwurfsbegründung zu entnehmende Regelungsintention besteht nicht darin, eine angemessene Abwägung vorzunehmen, sondern Sicherheitsaspekte besonders zu betonen und diesen damit insbesondere gegenüber dem allgemeinen Schutz vor **anlassloser Erfassung den Vorrang** zu geben. Letztendlich läuft der Entwurf darauf hinaus, dass in den genannten öffentlichen Räumen private Betreiber auf die Sicherheitsintention hinweisen können, wogegen in der Folge – auch durch Aufsichtsbehörden – nicht mehr argumentiert können werden soll. Damit werden die o. g. Erwägungen des BVerfG ad absurdum geführt. Die Regelung enthält keine Anforderung dahingehend, dass eine spezifische (terroristische oder anderweitig anschlagsbezogene) Gefährdungslage bestehen muss. Da an allen der genannten Plätze Anschläge nicht ausgeschlossen sind, wird damit Videoüberwachung immer gerechtfertigt. Davon geht auch der Entwurf aus, der an keiner Stelle besondere Schutzinteressen benennt, die einer Videoüberwachung noch entgegenstehen könnten. In der Praxis würde dies darauf hinauslaufen, dass öffentliche Plätze einer optischen Totalüberwachung unterworfen werden.

Keine polizeilichen Hilfsarbeiten

Die Regelung ist auch insofern problematisch, als zusätzlich zu der ursprünglichen Intention von (insbesondere privater) Videoüberwachung, etwa dem Schutz des Hausrechts oder eigener Sicherheitsinteressen, dieser ein eigenständiger öffentlicher Zweck, nämlich die Bekämpfung des Terrorismus und anderer schwerer Gewalttaten, zugemessen wird. Damit werden private Stellen gesetzlich zu Instrumenten der allgemeinen Gefahrenabwehr und zu **Informationsgehilfen der Polizei** gemacht. Die Gesetzesbegründung führt hierzu aus: „Damit stehen der Polizei und Staatsanwaltschaft verstärkt effektive Übersichts-, Aufklärungs- und Ermittlungsmöglichkeiten zur Verfügung“

(S. 6 des Entwurfs). Es geht dem Entwurf also nicht nur darum, nach einem Anschlag Ermittlungsmaterial für die Polizei zu beschaffen, sondern darüber hinausgehend die Betreiber von Videoüberwachungsanlagen zu veranlassen, ihre Kameras mit Systemen der Polizei zu koppeln und dadurch die Bilder „in Echtzeit" zur Verfügung zu stellen. Eine derartige Funktionalisierung Privater für Zwecke einer wie auch immer verstandenen öffentlichen Sicherheit, für die es derzeit keine gesetzliche Grundlage gibt, ist – auch im Hinblick auf die deutsche Geschichte, nicht nur im Nationalsozialismus, sondern auch in der DDR – hoch problematisch.

Die Notwendigkeit des Entwurfs wird mit den „Vorfällen in München und Ansbach im Sommer 2016" begründet. Es ist zutreffend, dass sich bei einer Änderung der Sicherheitssituation eine Änderung hinsichtlich der Abwägung zwischen Überwachung und Datenschutz ergeben kann. Die erwähnten Vorfälle sind aber für eine Gesetzesänderung keine Rechtfertigung. Es handelt sich um Einzelfälle; die Möglichkeit derartiger Anschläge ist schon seit vielen Jahren bekannt und wird auch seitdem bei der Interessenabwägung nach § 6b BDSG berücksichtigt. Es ist nicht angebracht, anlässlich einzelner Ereignisse Gesetze zu ändern, die flächendeckend und zeitlich unbegrenzt (siehe dazu aber unten) für die gesamte Bundesrepublik Deutschland gelten.

Der Gesetzentwurf berücksichtigt nicht, dass die genannten öffentlichen Orte auch solche sind, an deren in besonderem Maße das **Versammlungs- und Demonstrationsrecht** gemäß Art. 8 GG und Art. 12 GRCh wahrgenommen wird. Damit Menschen nicht wegen der Kameras von der Teilnahme abgehalten werden, müssten derartige Kameras bei friedlichen Versammlungen abgeschaltet werden. Dies ist jedoch nicht gewährleistet. (BVerfG NJW 1984, 422 – Volkszählung; OVG Münster, B. v. 23.11.2010 – 5 A 2288/09, DVBl 2011, 175 f.; VG Hannover U. v. 14.07.2014 – 10 A 226/13, DANA 2014, 134).

Beeinträchtigt wird zudem das aus der allgemeinen Handlungsfreiheit nach Art. 2 Abs. 1 GG abzuleitende Recht auf **unbeobachtete Mobilität**. Durch die Aufnahme von „Einrichtungen und Fahrzeugen des öffentlichen Personenverkehrs" wird generell ein Freibrief zur Erfassung dieser Räume geschaffen. Damit wird faktisch das Recht auf Anonymität bei der Nutzung öffentlicher Verkehrsmittel abgeschafft.

Verletzung der Verhältnismäßigkeit

Die geplante Regelung ist angesichts der Schwere des Eingriffs für die Allgemeinheit **nicht verhältnismäßig**. Zwar wird zu Recht behauptet, dass „die Ermittlungstätigkeit von Polizei und Staatsanwaltschaft … durch die Zurverfügungstellung von Videoaufzeichnungen erheblich erleichtert" werden kann (S. 4 des Entwurfs). Insofern kann eine Ausweitung der Videoüberwachung im öffentlichen Raum für den angestrebten Zweck als eine geeignete Maßnahme angesehen werden. Der Entwurf macht aber keinerlei Aussagen zur Erforderlichkeit und zur Angemessenheit und nimmt keine Abwägung vor. Insbesondere trifft er keinerlei Aussage zu den abzuwägenden Persönlichkeitsrechten. Eine Vielzahl von wissenschaftlichen Untersuchungen hat ergeben, dass eine Ausweitung von Videoüberwachung im öffentlichen Raum keine erkennbare Verbesserung der Sicherheitslage bewirkt (Nachweise z. B. in Hempel/Metelmann, Bild – Raum – Kontrolle, Videoüberwachung als Zeichen gesellschaftlichen Wandels, 2005; Töpfer, Videoüberwachung als Kriminalprävention? Plädoyer für einen Blickwechsel, *Kriminologisches Journal 2009*, 272 ff.; Hamburg Studie: Videoüberwachung bringt nichts, DANA 3/2010, 121; BReg. in BT-Drs. 17/2349: statistisch erfassbare wesentliche Kausalität „kaum darstellbar"). Dies gilt insbesondere, nachdem sich die Bereitstellung von Bildern aus dem öffentlichen Raum situationsbezogen zu Attentaten durch Handybesitzer massiv verbessert hat, so wie sich dies z. B. anlässlich des Anschlags auf den Boston-Marathon am 15.04.2013 gezeigt hat. Ein Blick in andere Staaten, in denen teilweise schon eine flächendeckende Videoüberwachung des öffentlichen Raums erfolgt, zeigt, dass dort (terroristische) Attentate durch die optische Überwachung nicht verhindert werden können. Dies gilt in besonderem Maße für islamistische terroristische Anschläge, die oft als Selbstmordattentate durchgeführt werden und bei denen potenzielle Täter oft mit hoher Professionalität vorgehen, sich von Überwachungsmaßnahmen nicht einschränken lassen und geeignete Gegenmaßnahmen (z. B. Vermeidung, Tarnung) ergreifen. Eine Erforderlichkeit der Regelung ist demnach nicht gegeben.

Überhaupt nicht verständlich ist die dringliche Behandlung des vorliegenden Entwurfes zur Änderung des Bundesdatenschutzgesetzes, das am 24.05.2018 voraussichtlich außer Kraft tritt bzw. nicht mehr anwendbar sein wird. Dies gilt insbesondere für die Regelungen zur Videoüberwachung, da insofern nach Wirksamwerden der **Europäischen Datenschutzgrundverordnung** (DSGVO) am 25.08.2018 kein nationaler gesetzlicher Regelungsspielraum mehr verbleibt (Roßnagel, Europäische Datenschutz-Grundverordnung, 2016, S. 52). In diesem Zusammenhang muss darauf verwiesen werden, dass seit vielen Jahren bestehende, an Relevanz zunehmende und auch nach dem 25.05.2018 bestehen bleibende Regelungsdefizite im deutschen Datenschutzrecht existieren, die vom Bundesinnenministerium bisher nicht erkennbar angegangen wurden oder werden (Netzwerk Datenschutzexpertise, Datenschutzrechtlicher Handlungsbedarf 2016 für die deutsche Politik nach Verabschiedung der EU-DSGVO, Stand 09.05.2016, http://www.netzwerk-datenschutzexpertise.de/sites/default/files/empf_2016_nat_regelungsbedarf.pdf). Der Eindruck ist nicht von der Hand zu weisen, dass mit dem Entwurf neben dem Versuch, bei der Videoüberwachung Datenschutzbelange hinter Sicherheitsinteressen massiv zurückzudrängen, im Hinblick auf die Bundestagswahl im Herbst 2017 sicherheitspolitische Symbolpolitik betrieben wird. Eine derartige Behandlung des BDSG und der damit verbundene Missbrauch der Gesetzgebung zeugen von einer Geringachtung des Grundrechts auf Datenschutz.

Wir raten daher dringend, von dem Gesetzgebungsvorhaben Abstand zu nehmen.

Pressemitteilung der GMDS/GDD

Datenschutzregelungen im Gesundheitswesen: „massiv überarbeitungsbedürftig“

Im einem 18-seitigen „Positionspapier zur Neugestaltung der datenschutzrechtlichen Regelungen bzgl. der Verarbeitung von personenbezogenen Daten in der Versorgung, Qualitätssicherung und Forschung im Gesundheitswesen“ vom 15.08.2016 haben die „Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.“ (GMDS), Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ und die „Gesellschaft für Datenschutz und Datensicherheit e. V.“ (GDD), Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“ den tatsächlichen und rechtlichen Regulierungsbedarf in Deutschland nach der Veröffentlichung der Europäischen Datenschutz-Grundverordnung (DSGVO) zusammengefasst.

Dieses Positionspapier untersucht, welche bisherigen Regelungsdefizite bestehen und wie diese unter Einbeziehung der DSGVO umgesetzt werden können. Dieses Positionspapier ist dem deutschen Bundestag bzw. den zuständigen Bundesministerien, aber auch der Landespolitik – da einige Gesetzgebungskompetenzen bei den Ländern liegen – ans Herz zu legen, damit endlich das Regelungschaos im Bereich des deutschen Gesundheitsdatenschutzes beendet wird.

Hier wird die Zusammenfassung abgedruckt:

„Die Patientenversorgung erfolgt heute institutions- und bundeslandübergreifend. Daher sollte die durch die Einführung der europäischen Datenschutzgrundverordnung (DSGVO) zu erfolgende Änderung der Gesundheitsdatenschutzgesetzgebung in Bund und Ländern dazu genutzt werden, diesem Umstand Rechnung zu tragen und die Gesetzgebung bzgl. des Gesundheitsdatenschutzes von Bund und Ländern harmonisieren.

Es ist zwingend notwendig, dass Erlaubnistatbestände zur Datenweitergabe an mitbehandelnde und/oder weiterbehandelnde Personen, die nicht zwangsläufig ärztliche Personen sein müssen, weiterhin gesetzlich geregelt bleiben. Dies schließt die derzeitigen gesetzlichen Regelungen der Sozialgesetzbücher ein, insbesondere auch die Regelungen bzgl. des MDK. Es ist wünschenswert, dass diese Erlaubnistatbestände nicht zwingend die Einwilligung des Patienten erfordern, wenngleich selbstverständlich die Transparenz gegenüber dem Patienten gewährleistet sein muss.

Die medizinische Forschung wird in der DSGVO nur am Rande betrachtet. Vielmehr überlässt man die gesetzliche Ausgestaltung dieses Themas dem nationalen Gesetzgeber. Damit der medizinische Forschungsstandort Deutschland nicht den Anschluss an die internationale medizinische Forschung verliert, benötigt Deutschland klare Regeln bzgl. des Umgangs mit Daten der besonderen Kategorien zu Forschungszwecken. Insbesondere werden gesetzliche Erlaubnistatbestände bzgl. des Umgangs mit Biomaterial benötigt, aber auch Regelungen für einrichtungsübergreifende Forschung und Qualitätssicherung mit den Daten der Patientenversorgung.

Neben der Forschung ist die Qualitätssicherung der medizinischen Versorgung unabdingbar. Auch hier müssen mindestens die aktuellen Regelungen beibehalten werden, welche die Nutzung von Daten der Routineversorgung zu Zwecken der Qualitätssicherung erlauben. Nicht staatlich geforderte Register sind für die Weiterentwicklung der Versorgung unverzichtbar, diese brauchen gesetzliche Erlaubnistatbestände.

In der heutigen Zeit ist die elektronische Datenverarbeitung derart komplex geworden, dass innerhalb einer verantwortlichen Stelle - wie einem Krankenhaus oder einer Arztpraxis - das dort beschäftigte Personal ohne externe Unterstützung die EDV-Prozesse nicht managen kann. Die Gesetzgebung sollte dem Rechnung tragen und ermöglichen, dass Daten außerhalb eines Krankenhauses verarbeitet werden dürfen und den Daten dort derselbe gesetzliche Schutz wie in der versorgenden Einheit gewährt wird.

Hinsichtlich der Bestellpflicht eines Datenschutzbeauftragten ist es wünschenswert, dass einerseits die bestehenden Regelungen in Deutschland beibehalten werden. Die Betroffenenrechte sind in der DSGVO sehr umfangreich ausgestaltet, was angesichts der immer stärkeren digitalen Vernetzung verständlich und begrüßenswert ist. Dennoch sollte der Gesetzgeber einige wenige dieser Rechte (siehe z. B. Kapitel 4.2.2) einschränken, bis nationale Umsetzungsvorgaben (z.B. im Rahmen des Rechts auf Datenübertragbarkeit) eine nutzbare Gestaltung dieser Betroffenenrechte erlauben. Art. 9 Abs. 3 DSGVO fordert eine Geheimhaltungspflicht für Personen, welche besondere Kategorien personenbezogener Daten gemäß Art. 9. Abs. 2 lit. h DSGVO verarbeiten. In verschiedenen juristischen Kommentaren werden verschiedene Kategorien von Personen genannt, die nicht unter den Schutzbereich des § 203 StGB fallen, sodass hier eine Regelung analog § 17 UWG oder eine Änderung des § 203 StGB selbst zur Herstellung einer Rechtssicherheit wünschenswert erscheint.“

Das gesamte Positionspapier ist im Internet unter https://www.gesundheitsdatenschutz.org/lib/exe/fetch.php/positionspapier.pdf abrufbar.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

vzbv mahnt erfolgreich Pokémon-Go-AGB ab

Der Verbraucherzentrale Bundesverband (vzbv) hatte den Pokémon-Go-Anbieter Niantic Mitte Juli 2016 abgemahnt. Er teilte am 24.10.2016 mit, dass das Unternehmen daraufhin seine Nutzungsbedingungen und die Datenschutzrichtlinien (Allgemeine Geschäftsbedingungen – AGB), die gegen deutsches Recht verstoßen, bis zum Jahresende 2016 in 15 Punkten nachbessern wolle. In der Datenschutzerklärung fanden sich bislang schwer verständliche oder zu weitreichende Einwilligungserklärungen. So konnten personenbezogene Daten nach Ermessen des Spielentwicklers an unbeteiligte Dritte weitergegeben werden. Gemäß der Mitteilung des vzbv hat Niantic zu allen beanstandeten Klauseln eine Unterlassungserklärung abgegeben. Bis zur Nachbesserung darf sich das Unternehmen nicht mehr auf die beanstandeten Klauseln berufen. Darin hatte es sich etwa auch vorbehalten, den mit dem Spieler geschlossenen Vertrag jederzeit abzuändern oder Dienste ganz einzustellen – ohne jede Rückerstattung von Geld, das etwa in In-App-Käufe geflossen ist. Ebenso kritisch waren die Nutzungsbedingungen, für die kalifornisches Recht gelten sollte und die weitreichende Haftungs- und Gewährleistungsausschlüsse enthielten (vgl. Appel und Spaeing, DANA 3/2016, 134 ff.; Pokémon Go: Niantic darf Nutzerdaten nicht mehr weitergeben. www.heise.de 24.10.2016).

Bund

vzbv mahnt WhatsApp ab

Das Marktwächter-Team vom Verbraucherzentrale Bundesverband (vzbv) hat WhatsApp abgemahnt, weil das Unternehmen persönliche Daten wie Telefonnummern an seinen Mutterkonzern Facebook weiterreichen will. Neue Nutzungs- und Datenschutzbestimmungen, die August 2016 vorgestellt wurden, sollen dies ermöglichen. Diese sind, so der vzbv, „zu großen Teilen" unzulässig. Weitergegeben wird u. a. die Handynummer an Facebook, unabhängig davon, ob die jeweilige Nutzende auch bei Facebook aktiv ist. Besonders kritisch sei, dass auch alle im Telefonbuch der WhatsApp-Nutzenden gespeicherten Nummern weitergegeben werden, also auch von Menschen, die WhatsApp überhaupt nicht verwenden. Bei der Übernahme von WhatsApp 2014 hatte Facebook öffentlich bekundet, dass der Dienst von WhatsApp unabhängig bleiben solle. Die VerbraucherInnen sollten also darauf vertrauen, dass ihre Daten allein bei WhatsApp bleiben und kein Datentransfer zu Facebook erfolgt. Facebook und Google beherrschen gemeinsam den globalen Online-Werbemarkt mit einem Marktanteil von ca. 80%. Die Daten des bisher werbefreien WhatsApp sollen künftig von Facbeook zur Vermarktung genutzt werden. Das Vertrauen der Nutzenden wurde enttäuscht. Der vzbv hatte bereits in seiner Abmahnung von Facebook Anfang 2015 erste Anzeichen für einen Datenaustausch kritisiert (Daten ohne Schutz: WhatsApp überschreitet rote Linie, www.vzbv.de 19.09.2016; WhatsApp abgemahnt, SZ 20.09.2016, 22).

Bund

Bald Vollverschleierungsverbot vor Gericht?

Bayern hat mit baden-württembergischer Unterstützung einen Antrag im Bundesrat eingebracht, der ein bundesweites Burka-Verbot in Gerichtsprozessen vorsieht. Bayerns Justizminister Winfried Bausback (CSU) will muslimische Frauen, die ihr Gesicht hinter einem Gesichtsschleier verbergen, per Gesetz dazu zwingen, bei Gerichtsverfahren ihr Antlitz zu enthüllen, wenn sie „Verfahrensbeteiligte" sind: Wenn die RichterInnen einer Zeugin nicht ins Gesicht sehen können, sei es ihnen regelmäßig auch nicht möglich, deren Aussagen umfassend zu würdigen oder auch nur ihre Identität eindeutig zu klären. „Auf die Wahrheit können wir in unserem Rechtsstaat aber nicht verzichten."

Die Burka und der Nikab-Gesichtsschleier widersprächen nicht nur dem in Deutschland vorherrschenden Verständnis von Gleichberechtigung und offener Kommunikation, so Bausback: „Vor Gericht erschweren sie maximal die Ermittlung der Wahrheit und die Durchsetzung von materieller Gerechtigkeit." Der baden-württembergische Justizminister Guido Wolf (CDU) verlangte: „Die Bundesregierung muss hier zügig für Rechtssicherheit sorgen und eine klare gesetzliche Regelung auf den Weg bringen." Bisher müssen die Gerichte im Einzelfall entscheiden, ob sie eine Abnahme dees Gesichtsschleiers anordnen und gegebenenfalls erzwingen (Bayern will Gesichtsschleier vor Gericht verbieten, www.handelsblatt.com 21.09.2016; Gegen Vollschleier vor Gericht, SZ 22.09.2016, 5).

Bund u. a.

Videoüberwachungskartierungsprojekt mit Openstreetmap

Mit dem Label „Surveillance under Surveillance" startete ein Kartografierungsprojekt, das Überwachungskameras weltweit anzeigt. Es visualisiert die Surveillance-Einträge von Openstreetmap, wobei es sich zumeist um Überwachungskameras handelt, die nicht auf der regulären Openstreetmap-Karte an-

gezeigt werden. Auf der Karte ist ersichtlich, ob es sich um klassische Kameras oder um Dome-Kameras handelt, die rundherum filmen können. Zudem wird erfasst, ob es sich um öffentliche Kameras, um Indoor-Kameras oder um Kameras handelt, die im Außenbereich hängen. Auch der Blickwinkel der Kameras kann eingetragen werden. So soll eine detaillierte Karte der mittlerweile fast überall präsenten Videoüberwachung entstehen.

Der Initiator des Projektes Max Kamba erläutert: „In unseren Städten gibt es kaum noch öffentlichen Raum, der nicht unter dauernder Beobachtung steht. Vielen scheinen die Kameras nicht mal aufzufallen und wenn doch, nicht zu stören. Dient ja der ´Sicherheit` und ´wer nichts zu verbergen hat…`. Um andere darauf hinzuweisen, wie schlimm es schon um das Thema Videoüberwachung bestellt ist, habe ich früher gerne auf das französische Projekt ´osmcamera` verlinkt, das genau wie Surveillance under Surveillance die weltweiten Surveillance-Einträge von Openstreetmap auf einer Karte dargestellt hat. Leider wurde die Seite kurz nach den Anschlägen auf die Konzerthalle Bataclan in Paris offline genommen. Das hat mich veranlasst, den noch auf Github verfügbaren Code zu forken und mit meinem eigenen Projekt an den Start zu gehen.

Die auf der Karte gezeigten Daten stellen aber nur ein sehr verzerrtes Bild der Situation dar. Abhängig vom Engagement einzelner bei Openstreetmap Aktiven sind Daten erfasst oder eben nicht. In Hannover, durch diverse Antikameraaktionen des AK-Vorrat bekannt, gibt es mit über 1.100 Einträgen z. B. mehr erfasste Kameras als in Berlin (knapp über 1000). Kassel hingegen ist ein weißer Fleck. Da scheint die Welt noch in Ordnung zu sein, was ich allerdings nicht glauben kann.“

Alle, die einen Openstreetmap-Account haben, können weitere Kameras erfassen oder bereits verzeichnete Kameras korrigieren und damit die Karte verbessern. Projekte zur Erfassung von Überwachungskameras gibt es schon lange. Viele arbeiteten nebeneinander her. Mit der Fokussierung des Projektes auf die Surveillance-Einträge bei Openstreetmap könnten nun erstmals die Erkenntnisse zusammengefügt werden (Reuter, Eine Weltkarte der Videoüberwachung, netzpolitik.org, 10.08.2016).

Baden-Württemberg

Polizei-Bodycams mit Prerecording

Mit den Stimmen von CDU, den Grünen, der FDP/DVP und der AfD hat der Landtag von Baden-Württemberg einen Gesetzentwurf verabschiedet, der die Nutzung von Bodycams durch die Polizei regelt. Dabei wird der Polizei bei dem auf sechs Monate befristeten Pilotprojekt in drei Testregionen das Prerecording gestattet. In einen gesonderten Flash-Speicher werden kontinuierlich jeweils 60 Sekunden aufgezeichnet, die erst bei einer aktivierten Aufnahme dauerhaft gespeichert werden. Die AfD hatte ein Prerecording von fünf Minuten gefordert, aber keinen eigenen Antrag gestellt. Die SPD hatte in ihrem Gesetzesvorschlag gefordert, auf das Prerecording ganz zu verzichten und damit den Bedenken des früheren Landesdatenschützers Lars Klingbeil entsprochen, der bei einer Anhörung von einer „massiven Datenspeicherung auf Vorrat“ gesprochen hatte.

Baden-Württemberg ist damit nach Hessen das zweite Bundesland, in dem die Bodycam mit dem umstrittenen Prerecording arbeitet. In Rheinland-Pfalz hat man sich gegen das Prerecording entschieden. In Hessen wurde das Prerecording nachträglich eingeführt; der Hessische Datenschutzbeauftragte hatte keine Bedenken. Dieses Verfahren, das beim Einsatz der Bodycams in Nordrhein-Westfalen und Hamburg verboten ist, zeichnet in einer Endlosschleife sechzig Sekunden lang auf und überschreibt diese Aufzeichnung kontinuierlich. Erst wenn der eigentliche Aufnahmeknopf der Bodycam gedrückt wird, werden die letzten sechzig Sekunden fest gespeichert. Auf sie kann weder der Video-Operator noch die mit Bodycams ausgerüstete Polizeistreife zugreifen, sondern nur ein Vorgesetzter mit einem besonderen Passwort.

In der abschließenden Aussprache vor der Gesetzesabstimmung betonte der grüne Abgeordnete Hans-Ulrich Sckerl, dass Bodycams „erwiesenermaßen“ geeignet seien, auf Angriffe auf Polizeibeamte durch Abschreckung zu unterbinden. Thomas Strobl (CDU), Minister für Inneres, Digitalisierung und Migration führte am Beispiel eines durch einen Messerangriff schwerverletzten Polizeibeamten aus, warum das Prerecording wichtig sein soll: In Extremsituationen müssten Polizisten handeln und könnten nicht auf die Aufnahmetaste drücken.

Die Bodycam soll in Baden-Württemberg bis zur Sommerpause 2017 getestet und wissenschaftlich evaluiert werden, ehe der Landtag über eine Dauerlösung abstimmt. Bislang gibt es keinen wissenschaftlich validen Nachweis zur Wirkung von Bodycams. Auch die Zweckgebundenheit des Prerecording ist noch nicht untersucht worden. Dies stellte Heiko Arnd, Leiter der Arbeitsgruppe Bodycam bei der rheinland-pfälzischen Polizei in einer Anhörung vor dem Landtag Nordrhein-Westfalens am 27. September fest.

Nach seinen Angaben zum Pilotprojekt kamen Bodycams in 8.290 Fällen in Rheinland-Pfalz zum Einsatz, wobei 591 Aufnahmen entstanden. Von diesen Aufnahmen wurden 192 dauerhaft gespeichert (von der automatischen Löschung nach zwei Wochen ausgenommen) und 97 der Staatsanwaltschaft als Beweismittel übergeben. Sein vorläufiges Fazit: „Ob die Bodycam eine präventive Wirkung hat, ist vor allem von der Wahrnehmungsfähigkeit des betroffenen Bürgers abhängig. Eine Reaktion findet jedoch grundsätzlich statt. Ist die Wahrnehmung des Betroffenen jedoch durch Alkohol-, Drogen- oder anderen Medikamentenkonsum beeinflusst, scheint die Bodycam ab einem bestimmten Grad keine Wirkung zu entfalten“ (Borchers, Baden-Württemberg beschließt Bodycam-Einführung mit Prerecording, www.heise.de 12.10.2016).

Bayern

Gesinnungsüberprüfung bei Richter-Bewerbungen geplant

Die bayerische Staatsregierung will künftig alle neuen RichterInnen vor ihrer Einstellung vom Verfassungsschutz überprüfen lassen. Mit ihrem Beschluss vom 27.09.2016 will das Kabinett die Wiederholung eines Vorgangs aus dem Jahr 2014 vermeiden, als ein aus Berlin zugezogener Rechtsradikaler im oberfränkischen Lichtenfels Amtsrichter geworden war. Der Neonazi in der bayerischen Richterrobe hatte 2014 bundesweit Schlagzeilen

gemacht – er war dem Brandenburger Verfassungsschutz als Protagonist des rechtsextremen Musikprojekts „Hassgesang“ bekannt. „Adolf Hitler, Sieg Heil tönt zu Dir empor“, soll der Mann getextet haben. Er hatte in Berlin Rechtswissenschaften studiert und dort auch sein Referendariat absolviert, bevor er als Zivilrichter in den bayerischen Staatsdienst wechselte. Die rechtsradikale Gesinnung des Mannes war vorab an die bayerischen Behörden übermittelt worden. Dennoch fiel die Vergangenheit des Richters erst nach Monaten und nur durch Zufall auf. Justizminister Winfried Bausback (CSU) ließ den Mann nach Bekanntwerden seiner extremistischen Aktivitäten unverzüglich aus dem Dienst entfernen.

Innenminister Joachim Herrmann (CSU) hatte anschließend eine Regelanfrage beim Verfassungsschutz für sämtliche neue BeamtInnen ins Spiel gebracht, was zu einer Überprüfung von alljährlich vielen Tausend Bewerbenden durch das Landesamt für Verfassungsschutz führen würde. Nun sollen nur RichterbewerberInnen überprüft werden. Justizminister Bausback erläuterte: „Das Richteramt ist ein besonders herausgehobenes und äußerst verantwortungsvolles Amt“. Der Staat müsse schon vor der Einstellung sicherstellen, „dass unsere künftigen Richterinnen und Richter mit beiden Beinen auf dem Boden des Grundgesetzes stehen“. Die Überprüfung soll erst erfolgen, nachdem das Vorstellungsgespräch positiv ausging und die Betroffenen ihre Einwilligung erteilt haben. Wer die Zustimmung verweigert, wird nicht eingestellt. Ulrike Grote von den Grünen kritisierte diesen „überzogenen Grundrechtseingriff“. Die Verbände dagegen reagierten positiv, etwa Rolf Habermann, Vorsitzender des Bayerischen Beamtenbunds: „Wir unterstützen alle Maßnahmen, die die Verfassungstreue im öffentlichen Dienst sicherstellen.“ Für den bayerischen Richterverein ist es wichtig, dass die Bewerbenden bei Zweifeln an ihrer Verfassungstreue gehört werden, so der Vorsitzende Walter Groß: „Wir sind überzeugt, dass die Verfassungstreue von Richtern und Staatsanwälten gewährleistet sein muss“ (Verfassungsschutz soll neue Richter in Bayern überprüfen, www.nordbayern.de 23.09.2016; Verfassungsschutz soll neue richter überprüfen, SZ 28.09.2016, 30).

Nordrhein-Westfalen

Ausländerbehördenmitarbeiter wegen Spionage für Indien verdächtigt

Ein 58-jähriger deutscher Mitarbeiter der Ausländerbehörde Ostwestfalen soll in Deutschland lebende indische Staatsangehörige ausspioniert haben. Sein Auftraggeber sei ein indischer Geheimdienst gewesen. Er wurde Februar 2016 wegen dringendem Tatverdacht festgenommen und in Untersuchungshaft gebracht. Die Bundesanwaltschaft führte ihn am 21.09.2016 dem Ermittlungsrichter des Bundesgerichtshofs wegen „geheimdienstlicher Agententätigkeit und Verletzung des Dienstgeheimnisses in 45 Fällen“ vor. Der Geheimdienst soll vor allem an Informationen über oppositionelle und extremistische Sikhs interessiert gewesen sein. Diese soll sich der Beschuldigte über seine Zugänge zu amtlichen Registern selbst beschafft haben. Der Tatverdächtige habe die gesammelten Informationen tatsächlich an den indischen Nachrichtendienst weitergegeben. Sowohl Privaträume als auch die Diensträume des Beschuldigten wurden durchsucht (Mutmaßlicher Agent festgenommen, www.tagesschau.de 17.09.2016; Der indische Spion, SZ 21.09.2016, 5).

Hamburg

Caspar verbietet Facebook die Entgegennahme von WhatsApp-Daten

Hamburgs Datenschutzbeauftragter (HmbBfDI) Johannes Caspar hat Ende September 2016 Facebook mit sofortiger Wirkung untersagt, Daten von deutschen WhatsApp-Nutzenden zu erheben und zu speichern. Zudem müsse Facebook bereits von WhatsApp übermittelte Daten löschen. Die rund 35 Millionen WhatsApp-AnwenderInnen in Deutschland müssten selbst entscheiden können, ob sie eine Verbindung ihres Kontos mit Facebook wünschen, so Caspar: „Dazu muss Facebook sie vorab um Erlaubnis fragen. Dies ist nicht geschehen.“ Facebook kündigte an, gegen die Anordnung Rechtsmittel einzulegen.

WhatsApp hatte zuvor im August angekündigt, künftig die Nutzerdaten des Dienstes an Facebook weiterzugegeben. WhatsApp teilt der Konzernmutter die Inhalte der Adressbücher mit Telefonnummern mit sowie auch Informationen darüber, wie häufig der Kurzmitteilungsdienst genutzt wird. Betroffen von dem Austausch sind also nicht nur die Nutzenden selbst, sondern auch deren Kontakte. WhatsApp-Mitglieder konnten zwar der Verwendung ihrer Daten für die Personalisierung von Facebook-Werbung und Freunde-Vorschläge widersprechen. Die Telefonnummern werden allerdings in jedem Fall mit Facebook geteilt, wenn jemand die App weiter nutzen will.

Der HmbBfDI argumentiert, Facebook und WhatsApp seien selbstständige Unternehmen, welche die Daten ihrer Nutzenden jeweils auf Grundlage ihrer Nutzungs- und Datenschutzbedingungen verarbeiten. Nach dem Erwerb von WhatsApp durch Facebook vor zwei Jahren hatten deren Chefs Mark Zuckerberg und Jan Koum zugesichert, dass Daten der Nutzenden nicht untereinander ausgetauscht würden. Koum im Jahr 2014: „Das wird sich für euch, unsere Benutzer, ändern: nichts“. Keine Anzeigen, Silicon-Valley-Ehrenwort: „Du kannst Dich absolut darauf verlassen, dass deine Kommunikation nicht durch Werbung gestört wird.“ Caspar: „Dass dies nun doch geschieht, ist nicht nur eine Irreführung der Nutzer und der Öffentlichkeit, sondern stellt auch einen Verstoß gegen das nationale Datenschutzrecht dar“. In den zwei Jahren hat WhatsApp seine Nutzerzahl auf mehr als eine Milliarde verdoppelt.

Eine Sprecherin von Facebook behauptete dagegen, dass sich das soziale Netzwerk an europäisches Datenschutzrecht halte: „Wir sind offen, mit der Hamburger Datenschutzbehörde zusammenzuarbeiten, um ihre Fragen zu klären und Bedenken auszuräumen“. Auf eine Beendigung des Datenaustauschs zwischen WhatsApp und Facebook wollten sich die Unternehmen nicht einlassen.

Facebook hat nun die Möglichkeit, Widerspruch einzulegen, der allerdings keine aufschiebende Wirkung hat, da die sofortige Vollziehbarkeit angeordnet wurde. Hiergegen kann und wird Facebook beim

Verwaltungsgericht vorgehen. Sollte das soziale Netzwerk der vollstreckbaren Anordnung nicht folgen, kann der HmbBfDI ein Zwangsgeld in Höhe von bis zu 1 Mio. Euro verhängen.

Wegen des gleichen Vorgangs hatte zuvor die Verbraucherzentrale Bundesverband (vzbv) von WhatsApp eine Unterlassungserklärung gefordert. Die Facebook-Tochter hat aber die ihr gesetzte Frist verstreichen lassen, so dass nun auch der vzbv zivilrechtlich gegen den Datenaustausch vorgehen wird (s. o.).

Der HmbBfDI hatte in der Vergangenheit bereits mehrfach versucht, gegen Datenschutzverstöße von Facebook vorzugehen. Zuletzt wollte er durchsetzen, dass Facebook auch Anmeldungen unter einem Pseudonym zulässt, scheiterte aber vor der Verwaltungsgerichtsbarkeit in Hamburg (DANA 3/2016, 154 f.). Das Gericht hatte Caspar an die Niederlassung von Facebook in Irland verwiesen, die das soziale Netzwerk in Europa betreibt (Hurtz, Verkauft und verraten, SZ 22.09.2016, 19; Kannenberg, Datenschutzbeauftragter verbietet Facebook WhatsApp-Datenabgleich, www.heise.de 27.09.2016, HmbBfDI, Anordnung gegen Massendatenabgleich zwischen WhatsApp und Facebook, 27.09.2016; Hurtz, Allein gegen Facebook, SZ 28.09.2016, 5).

Datenschutznachrichten aus dem Ausland

Weltweit

PI veröffentlicht Surveillance Industry Index

Privacy International (PI) hat seinen „Surveillance Industry Index" überarbeitet und deutlich ausgebaut und listet nun 42 deutsche Firmen auf, die Überwachungstechnik verkaufen. Deutschland gehört hinter den USA, Großbritannien und Frankreich sowie vor Israel zu den „Top 5" der Nationen mit den weltweit die meisten Herstellern und Exporteuren. Die Bürgerrechtsorganisation PI hat den Index am 02.08.2016 gemeinsam mit dem Projekt Transparency Toolkit ins Netz gestellt. Zu den 42 deutschen Firmen, die Systeme verkaufen, mit denen sich Telekommunikation abhören, Computer mit Trojanern heimlich durchsuchen, Nutzer von Mobiltelefonen verfolgen oder soziale Netzwerke auswerten lassen, gehören Elaman, Ipoque, Gten, DigiTask, Cognitec Systems, Utimaco, Secunet, Syborg, Siemens, Rohde und Schwarz, Rheinmetall oder FinFisher. Fünf davon haben ihren Hauptsitz in München. Eine Übersicht zu den belieferten Ländern gibt es auf Netzpolitik.org.

Nach den Snowden-Enthüllungen 2013 brachte PI erstmals mit seinem Index mehr Licht ins Dunkel der privaten Überwachungshelfer. Die Datenbank enthielt damals 338 Unternehmen aus 36 Ländern. Die zivilgesellschaftliche Institution entschied sich aber, die Webseite wieder offline zu nehmen, nachdem sie einen Fehler in der ihr zugrundeliegenden Drupal-Software entdeckt hatte. Nun sind 528 Unternehmen im Verzeichnis; es ist komplett durchsuchbar und soll regelmäßig aktualisiert werden. Die Informationen über 600 einzelne Exporte spezifischer Überwachungsprodukte mit Angaben auch zu den Einkaufsländern stammen aus offen verfügbaren Quellen einschließlich investigativer und technischer Analysen sowie aus staatlichen Export-Datenbanken. Berücksichtigt sind rund 1.500 Verkaufsbroschüren und vergleichbares Material, mit dem die Firmen nicht nur in autoritären Regimen um Kundschaft buhlen. Für den ursprünglichen Index hatte PI unter anderem die von Wikileaks veröffentlichten Spy Files ausgewertet.

PI veröffentlichte zudem einen Bericht über die globale Überwachungsindustrie. 87% der Unternehmen aus der Datenbank sitzen demnach in den OECD-Mitgliedstaaten, 75% in Nato-Ländern. Einen genaueren Blick werfen die Verfasser auf die Aktivitäten dieser Firmen in Deutschland, Italien, Großbritannien, Israel und den USA. Sie analysieren 152 gemeldete Importe von Überwachungstechnik in den Nahen Osten und Nordafrika.

Die ermöglichten Einblicke in eine sehr auf Geheimhaltung bedachte Industrie sind gemäß Edin Omanovic von PI wichtig, um die Beteiligten zur Rechenschaft ziehen und umfassenden, auch politischen Schutz entwickeln zu können. M. C. McGrath vom Transparency Toolkit bezeichnete die Datenbank als wertvolle Ressource für JournalistInnen, AktivistInnen, Forschende oder PolitikerInnen. Mit den vielfältigen Filtermethoden lasse sich rasch selbst herausfinden, mit welchen Überwachungsmitteln man möglicherweise ausgespäht wird. Eine ähnliche Datenbank hatte schon Andy Müller-Maguhn unter Bugged Planet ins Leben gerufen.

In einer Stellungnahme zu der Veröffentlichung stellte Secunet fest, dass die Firma weder Systeme zum Abhören noch Trojaner zum heimlichen Durchsuchen von Computern oder ähnliche Software herstellt. Secunet wird in der PI-Datenbank im Zusammenhang mit Counter-Surveillance-Techniken erwähnt (Krempl, Neue Datenbank beleuchtet die globale Überwachungsindustrie, www.heise.de 02.08.2016).

Belgien

Bahnkundschaft soll identifiziert werden

Die belgische Regierung plant, Daten von Nutzenden aller öffentlichen Verkehrsmittel zu erheben, mit denen das Land erreicht werden kann, also neben Flugzeugen auch Bahnen, Busse und Schiffe. Das würde wohl bedeuten, dass sich die KundInnen vor Abfahrt beim Ticketkauf am Schalter, am Kartenau-

tomaten oder im Internet erst persönlich ausweisen müssten. Der Terrorismus hat schon heute Folgen für die Freiheit und die Mobilität der Menschen in Europa: Im Flugverkehr sollen von 2018 an in allen Staaten ausführliche Daten der Passagiere registriert und monatelang gespeichert werden. Dies soll dann in Belgien vor allem auch für den Bahnverkehr gelten.

Die Bahn-Unternehmen in Europa reagierten alarmiert, so z. B. die Deutsche Bahn: „Das diskutierte Gesetz hätte weitreichende Auswirkungen auf den Eisenbahnverkehr zwischen Deutschland und Belgien und würde die Freizügigkeit unserer Kunden infrage stellen.“ Der Europäische Eisenbahnverband CER schrieb einen Protestbrief an Belgiens Premier Charles Michel, dessen Innenminister Jan Jambon von der flämisch-separatistischen N-VA den Plan forciert. Es seien gerade die Flexibilität und der offene Zugang, die das Bahnfahren attraktiv machten. Die Datenerhebung und Kontrolle wären derart aufwendig, dass dadurch KundInnen vertrieben und zum Ausweichen auf das Auto veranlasst würden. Außerdem liefen die Pläne dem Schengener Abkommen über grenzfreies Reisen in Europa zuwider.

Die Regierungsvorlage, über die das Parlament im Oktober 2016 diskutierte, geht auf die Anschläge von Brüssel im März 2015 zurück. Eine Sprecherin Jambons erläuterte: Terroristen wählten den Weg des geringsten Widerstands. Deshalb müssten alle Verkehrsmittel Richtung Belgien erfasst werden. Allerdings würden von den Bahnen weniger Daten angefordert als von Fluggesellschaften. In der EU-Kommission ist man nicht glücklich über die belgischen Pläne, kann und will aber nicht verhindern, dass Staaten zu solchen Maßnahmen greifen. Eine Studie zum Thema Bahn und Sicherheit vom November 2016 untersucht das Phänomen. Im EU-Parlament sind die Reaktionen unterschiedlich geteilt. Der Grüne Jan Philipp Albrecht fragte: „Ist es sinnvoll, immer mehr Daten über Lebensumstände zu sammeln, die in keinem Zusammenhang mit dem Risiko stehen?“ Der CDU-Abgeordnete Axel Voss hingegen erklärte, er wolle sich einer entsprechenden Diskussion nicht verwehren (Kirchner, Gläserne Waggons, SZ 01.-03.10.2016, 11).

Schweiz

Referendum erfolgreich für mehr Geheimdienstbefugnisse

Bei einem Referendum am 25.09.2016 hat sich eine klare Mehrheit der schweizer Abstimmungsberechtigten für die Ausweitung der Überwachungsbefugnisse des nationalen Geheimdienstes entschieden. Bei einer Stimmbeteiligung von ca. 42% haben 65,5% für ein vom Parlament bereits gebilligtes Gesetz gestimmt, das es dem Nachrichtendienst des Bundes (NDB) zur Abwehr von Terroranschlägen in Einzelfällen und bei begründetem Verdacht erlaubt, Telefonate abzuhören, Wohnungen zu verwanzen und Internetaktivitäten zu verfolgen. Das Gesetz war bereits vor einem Jahr verabschiedet worden, kam aber noch nicht in Kraft, da es durch das Referendum bestätigt werden musste.

GegnerInnen des Gesetzes beklagen, dass dadurch die Bürgerrechte stark eingeschränkt werden. Durch die Maßnahme könne Terrorismus kaum verhindert werden. Die offizielle Neutralität der Schweiz werde durch das Gesetz untergraben. Derzeit dürfen die Schweizer Behörden lediglich öffentlich verfügbare Informationen oder Tipps von ausländischen Behörden nutzen, wenn sie Bedrohungslagen innerhalb der Schweiz beobachten. Die BefürworterInnen machten geltend, dass der Geheimdienst mehr Möglichkeiten haben müsse, um bereits die Planungen für etwaige terroristische Anschläge zu erkennen und dadurch zu unterbinden. Die Schweiz müsse den Anschluss an andere Länder finden, um gegen Cyberkriminalität, Spionage und Extremismus zu kämpfen. Die vorgesehenen Eingriffe in Grundrechte seien auf einige wenige und zudem klar begründete Verdachtsfälle beschränkt. Vor solchen Überwachungen müsse schließlich stets die Zustimmung von Regierungsstellen und des Verwaltungsgerichtes eingeholt werden.

Amnesty International kritisierte das Ergebnis der Abstimmung. Das neue Gesetz ermögliche „unverhältnismäßige Überwachungsmaßnahmen“ und stelle eine Bedrohung für die Privatsphäre und die Meinungsäußerungsfreiheit dar. Patrick Walder, Kampagnenkoordinator von Amnesty International Schweiz meinte: „Dass die Mehrheit der Stimmberechtigten dem Nachrichtendienstgesetz zugestimmt hat, zeigt wohl, dass die Angst vor Terroranschlägen auch in der Schweiz überwiegt“. Er bezweifle, dass mehr Überwachung automatisch auch mehr Sicherheit bringe (Schweizer stimmen für mehr Überwachung, www.zeit.de 25.09.2016).

USA

Yahoo soll US-Behörde Zugriff auf alle E-Mail gewährt haben

Unter der Führung von Marissa Mayer entwickelte Yahoo 2015 eine neue Software, mit der alle für Yahoo-KundInnen eintreffenden E-Mails nach einer bestimmten Zeichenfolge durchsucht wurden. Yahoo hatte Presseberichten zufolge eine geheime Anordnung eines US-Geheimdienstes erhalten, alle für KundInnen eingehende E-Mails in Echtzeit zu scannen. Seit April 2015 wurden danach Treffer umgeleitet und so gespeichert, dass der Geheimdienst online darauf zugreifen konnte. Es ist der erste bekannt gewordene Fall dieser Art. Bisher wurden zwar regelmäßig die in einzelnen Mailboxen gespeicherten Daten gesichtet oder eine kleine Anzahl von Mailboxen überwacht, aber von einer umfassenden Überwachung durch einen Provider war noch nichts bekannt.

Ob Yahoo noch immer scannt, ist nicht bekannt. Die Anordnung soll vom FBI stammen, der im Inland regelmäßig im Auftrag der NSA tätig wird. Die Möglichkeit, gegen die geheime Anordnung vor Gericht zu gehen, soll Mayer nicht genutzt haben, was mehrere hochrangige Yahoo-Manager verärgert haben soll. Die Abteilung von Sicherheitschef Alex Stamos soll auf Mayers Geheiß komplett umgangen worden sein. Vielmehr programmierte die E-Mail-Abteilung die neue Software und installierte sie, ohne die Security-KollegInnen mit einzubeziehen. Einige Wochen danach soll die Sicherheitsabteilung die nicht von ihr autorisierte Software gefunden und für das Resultat eines Hacks gehalten haben.

Das Programm soll zudem nicht sauber programmiert worden sein, so dass die zum Abruf durch den Geheimdienst online gespeicherten E-Mails schlecht gesichert waren und Hacker darauf hätten zugreifen können. Yahoo musste jüngst eingestehen, dass Hacker 2014 Profilinformationen von mindestens 500 Mio. Nutzenden erbeutet haben. Stamos kündigte Yahoo im Juni 2015 und wurde Facebooks Sicherheitschef.

Der Transparenzbericht für das erste Halbjahr 2015 von Yahoo verschweigt die Arbeit für den US-Geheimdienst. Dort heißt es, dass 8424 Konten von US-Regierungsanfragen betroffen waren („Total Government Specified Accounts"). Auch im Transparenzbericht für das zweite Halbjahr, der das erste Halbjahr mit einschließt, berichtet Yahoo nur von 9373 betroffenen Konten. Wenn tatsächlich alle Yahoo-Konten überwacht worden sind, hätten hier Hunderte Millionen Konten genannt werden müssen. Eine Version von US-Regierungsbefehlen, die National Security Letters (NSL), werden mit sechs Monaten Verzögerung statistisch erfasst. NSL dürfen sich aber nicht auf den Inhalt von Kommunikation beziehen.

Ob juristischer Widerstand seitens Yahoo gefruchtet hätte, ist nicht abschätzbar, zumal die vom Geheimdienst genutzte Rechtsgrundlage nicht bekannt ist. Mayer rechnete dem Bericht zufolge mit einer Niederlage vor Gericht. Das Begehren des Geheimdienstes war extrem weit gefasst. Und Yahoo sollte nicht bloß Daten herausgeben, es musste neue, nicht-triviale Software schreiben, um dem Begehren überhaupt entsprechen zu können. Dieser Zwang könnte gegen den ersten sowie den fünften Zusatzartikel der US-Verfassung verstoßen. Apple hatte sich Ende Februar 2016 vor einem New Yorker Bundesbezirksgericht erfolgreich dagegen gewehrt, eine neue Variante von iOS zur Erleichterung der Überwachung programmieren zu müssen. Die Staatsanwalt hatte zunächst gegen diese Niederlage Berufung eingelegt, dann aber diesen Antrag zurückgezogen und damit ein Urteil in einem Präzedenzfall vermieden (DANA 2/2016, 99 ff.).

Die US-amerikanische Konkurrenz von Yahoo distanzierte sich deutlich vom Vorgehen des Unternehmens. Google und Apple versicherten, nie eine entsprechende Aufforderung bekommen zu haben. Ansonsten hätte man sich geweigert beziehungsweise wäre vor Gericht dagegen vorgegangen. Microsoft erklärte ebenso, nie solch eine Überwachungsaufforderung erhalten zu haben. Auch Facebook – wo der damals bei Yahoo offenbar übergangene Ex-Sicherheitschef Alex Stamos inzwischen arbeitet – versicherte, eine solche Aufforderung nie erhalten zu haben und dass die sonst auch bekämpft worden wäre. Ein Sprecher von Twitter gab das gleiche der Presse zu Protokoll. Dem steht das offizielle Statement von Yahoo gegenüber, in dem es heißt: „Yahoo ist ein gesetzestreues Unternehmen und hält sich an die Gesetze der Vereinigten Staaten." Ein Dementi der ursprünglich auf Basis zweiter anonymer Quellen erhobenen Vorwürfe sähe wohl anders aus.

Die NSA, der britische GCHQ und andere westliche Geheimdienste greifen in großem Umfang internationale Kommunikation ab, spionieren Unternehmen sowie staatliche Stellen aus und verpflichten Dienstleister im Geheimen zur Kooperation. Einzelheiten dieses totalen Überwachungssystems enthüllen streng geheime Dokumente, die der Whistleblower und ehemalige NSA-Analyst Edward Snowden an sich gebracht und 2013 an Medien weitergegeben hat.

Die Kritik an dem Vorgehen richtete sich so auch gegen die US-Regierung. Die Electronic Frontier Foundation (EFF) kommt zu dem Schluss, dass die E-Mail-Überwachung – sollte sie so stattgefunden haben – gegen die US-Verfassung verstößt. Zum ersten Mal sei von einer derartigen Überwachungsverfügung auch ein Diensteanbieter betroffen. Das Vorgehen richte sich auch gegen US-BürgerInnen, die vor einer derartigen Überwachung eigentlich geschützt seien. Yahoo habe in diesem Fall offenbar selbst geholfen und dabei unter Umständen sogar neue Sicherheitslücken geschaffen. Patrick Toomey von der American Civil Liberties Union (ACLU) bezeichnete die Enthüllung als „zutiefst verstörend". Offenbar habe die US-Regierung Yahoo zu einer generellen und verdachtslosen Überwachung verpflichtet, die der vierte Zusatzartikel der US-Verfassung verbiete. Die KundInnen würden darauf setzen, dass sich Unternehmen gegen solch ein Vorgehen vor Gericht wehren. Genau wie die EFF weist er darauf hin, dass die Anordnung offenbar unter Rückgriff auf Artikel 702 des Foreign Intelligence Surveillance Act formuliert wurde. Der müsse endlich reformiert werden oder der US-Kongress dürfe ihn Ende 2016 nicht verlängern (Holland, E-Mail-Scanning bei Yahoo: Google, Apple & Co. bestreiten, bei Überwachung geholfen zu haben, www.heise.de 05.10.2016; Sokolov, Alle Mails gescannt: Yahoo arbeitete für Geheimdienste, www.heise.de 05.10.2016; Yahoo unter Verdacht, SZ 06.10.2016, 19).

USA

Eine halbe Milliarde Yahoo-Konten gehackt

Bei Yahoo wurden Ende 2014 Daten von mehr als 500 Millionen Usern abgegriffen. Das Unternehmen teilte dies am 22.09.2016 über Sicherheitschef Bob Lord mit und äußerte die Vermutung, dass dahinter ein „staatlich finanzierter" Angreifer steckt: „Wir haben bestätigt, dass Ende 2014 eine Kopie bestimmter Nutzerkontoinformationen aus dem Netzwerk der Firma gestohlen wurde". Mit mindestens 500 Millionen betroffenen Konten inclusive Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten, und Passwort-Hashes handelt es sich, gemessen an der Zahl der Opfer, um den größten bekannt gewordenen Hack der IT-Geschichte. Vorangegangen waren u. a. Hacks auf Tumblr (65 Mio.), Linkedin (117 Mio.), Myspace (360 Mio.). Unglücklicherweise kommen bei Yahoo, so das Unternehmen „in manchen Fällen" noch verschlüsselte oder unverschlüsselte (!) Sicherheitsfragen und -antworten dazu. Bankverbindungen und Kreditkartendaten sollen nicht betroffen sein. Lord: „Die Untersuchung hat keine Beweise erbracht, dass der staatlich finanzierte Akteur derzeit in Yahoos Netz ist". Bei der Aufklärung arbeite Yahoo mit den Strafverfolgungsbehörden zusammen. Im August 2016 waren im Netz 200 Mio. Yahoo-Datensätze feilgeboten worden.

Yahoo informierte seine User per E-Mail und wies darauf hin, dass diese Nachrichten nicht zum Klicken von Links oder zum Öffnen von Anhängen auffordern. Die Opfer sollen umgehend ihre Passwörter ändern. Gleiches emp-

fiehlt Yahoo allen seinen Nutzern, die ihr Passwort seit 2014 nicht mehr geändert haben. Die unverschlüsselt gespeicherten Sicherheitsfragen und -antworten funktionieren nicht mehr. Der Konzern riet: „Überprüfen Sie Ihre Konten auf verdächtige Aktivitäten".

Im Unterschied zu den USA spielt Yahoo und beispielsweise sein Maildienst in Deutschland eigentlich keine große Rolle mehr. Allerdings sind auch zu Yahoo gehörende Dienste wie Flickr und Tumblr nur mit einem Yahoo-Account zu verwenden.

Der Datendiebstahl wurde zu einem für den Konzern ungünstigen Zeitpunkt bekannt, da der Telekom-Konzern Verizon diesen übernehmen will. Verizon erklärte, man werde die Situation ausgehend aus den Interessen des eigenen Unternehmens sowie der Kunden und Aktionäre prüfen. Der Telekom-Riese sei erst zwei Tage vor der öffentlichen Bekanntmachung von dem Datendiebstahl unterrichtet worden und verfüge zunächst nur über eingeschränkte Informationen. Die Yahoo-Übernahme für rund 4,8 Milliarden Dollar war im Juli vereinbart worden.

Unklar blieb bisher, seit wann genau Yahoo von dem gewaltigen Datendiebstahl wusste. Nach Presseinformationen hatte das Unternehmen schon im Juli 2016 Hinweise. In einer Pflichtmitteilung zum Verizon-Deal hatte Yahoo noch am 09.09. erklärt, dem Unternehmen sei kein Diebstahl von Nutzerdaten bekannt (Sokolov, Rekordhack bei Yahoo: Daten von halber Milliarde Konten kopiert, www.heise.de 22.09.2016; Hurtz, Der größte Hack der Welt, SZ 24./25.09.2016, 27).

USA

Klage gegen datensammelnde Vibrator-App

Die Benutzerin eines Online-Vibrators aus dem US-Staat Illinois verklagt in den USA den Hersteller von We-Vibe, die kanadische Firma Standard Innovation, weil diese über eine App höchstpersönliche Daten über den Einsatz des Masturbationsgerätes sammelt. Das teure Sexspielzeug kann nur mit einer bestimmten App voll ausgekostet werden; eine etwas günstigere Variante ist sogar „App-Only". Diese App „We-connect" überträgt intime Details an die Server des Herstellers. Die Klägerin beschuldigt Standard Innovation, das verheimlicht, und die Kundinnen so hinters Licht geführt zu haben. Die App muss auf einem Smartphone installiert werden, das über Bluetooth mit dem We-Vibe verbunden wird. Aus einer Vielzahl von vorgegebenen oder selbst kreierten Vibrationsmustern kann gewählt werden. In der Klage heißt es: „Die Beklagte hat We-Connect so programmiert, dass [die App] heimlich intime Details über die Nutzung des We-Vibe sammeln, darunter Datum und Zeit jeder Nutzung, [Vibrationsintensität], Vibrationsmodus oder -muster […] und, unglaublicherweise, die E-Mail-Adresse […], was die Beklagte die Verbindung der Nutzungsdaten mit einem bestimmten Kundenkonto ermöglicht". We-Connect ermöglicht außerdem einem Partner, mit der Benutzerin über Chat und Video in Verbindung zu treten. Sie kann dem Partner auch die Steuerung des Sexspielzeugs überlassen. Diese Funktion nennt Standard Innovation „connect lover" und wird als „sichere Verbindung zwischen Ihren Smartphones" beworben. Tatsächlich werden die intimen Unterhaltungen aber ebenfalls über die Server des Herstellers geroutet.

Die Klägerin, die zum Schutz ihrer Privatsphäre unter ihren Initialen N. P. auftritt, möchte ihre Klage als Sammelklage für alle gleichermaßen betroffenen Nutzerinnen in den USA respektive Illinois zugelassen sehen. Außerdem hat sie ein Verfahren vor Geschworenen beantragt. Begehrt wird eine Unterlassungsverfügung gegen Standard Innovation, Rückzahlung des vollen Kaufpreises, Schadenersatz und Strafschadenersatz. Die heimliche Datensammelei ohne Zustimmung der Betroffenen verletze ein Anti-Überwachungsgesetz auf Bundes- und eines auf Staatenebene, ein Verbraucherschutzgesetz in Illinois und stelle außerdem ein illegales Eindringen in die Privatsphäre dar. Der Hersteller bestreitet die Sammlung der Daten nicht. Es sei gängige Praxis, die Daten nicht personenbezogen auszuwerten. Die Server seien nicht gehackt worden. Und die Registrierung mit E-Mail-Adresse sei optional. Nach Presseberichten erklärte der Hersteller, er wolle künftig seine Verfahrensweisen mit den Daten „besser kommunizieren" (Sokolov, Klage gegen neugierige Vibrator-App, www.heise.de 16.09.2016).

Kuweit

DNA-Datenbank für Bevölkerung und Einreisende geplant

Das Emirat Kuweit will 400 Mio. $ in eine gigantische Datenbank investieren, um angeblich der Terrorgefahr zu begegnen. Darin sollen die genetischen Fingerabdrücke aller BewohnerInnen des Emirats, also 1,3 Mio. Staatsangehörige sowie 2,9 Mio. dort ständig lebende AusländerInnen, hinterlegt werden: Außerdem sollen auch Geschäftsreisende und TouristInnen DNA-Proben vor der Einreise abgeben.

Nachdem ein Anhänger der Terrormiliz Islamischer Staat (IS) vor einer schiitischen Moschee eine Bombe gezündet und 27 Menschen in den Tod gerissen hatte, beschloss das Parlament von Kuweit im Juli 2015 ein entsprechendes, vom Innenministerium vorbereitetes Gesetz. Mit der Datenbank soll künftig Verdächtigen die Einreise erschwert werden, und sie soll Opfer schneller identifizieren helfen, wenn es dennoch zu Anschlägen kommt. Als eigentlichen Grund hinter der Maßnahme wird von vielen vermutet, dass Kuwait die im Emirat lebenden Nachfahren von Beduinen loswerden möchte, die als Staatenlose am Rande der Gesellschaft leben. Über DNA-Tests könnte man ihnen nachweisen, dass ihre Abstammung keine kuwaitische ist, und sie so dauerhaft von Sozialleistungen ausschließen oder gar ausweisen.

Nachdem ein Jahr lang wenig geschah, hieß es im September 2016, das Gesetz werde „noch diesen Sommer", „bald" oder gar „sehr bald" umgesetzt. Die kuwaitische Botschaft in Berlin machte dazu keine näheren Angaben. Institutionen versuchten derweil, das Vorhaben noch zu stoppen: Der UN-Menschenrechtsausschuss rief Kuwait im Juli 2016 auf, das Gesetz zu ändern; er fürchtet, das Beispiel könnte auch anderswo Schule machen. Die Europäische Gesellschaft für Humangenetik

wandte sich Anfang September 2016 mit einem offenen Brief an das Emirat: In einem Land mit so strengen Gesetzen etwa zum Ehebruch könnten obligatorische DNA-Tests zu Verwerfungen führen; z. B. weil die DNA von Kindern und Vätern wohl nicht in jedem Fall zueinanderpassen dürfte. Die WissenschaftlerInnen befürchten, die Daten könnten durch Hacker oder einen Umsturz in falsche Hände geraten.

Kuwait wäre der erste Staat mit einer solchen Datenbank, die Folgen zeitigt, bevor sie eingerichtet ist. Die Presse vor Ort berichtet von einem seit kurzem anhaltenden Abwärtstrend bei Immobilienpreisen und zitiert Makler, die Villen und Luxuswohnungen zu Schleuderpreisen anbieten. Deren Eigentümer wollen das Emirat so schnell wie möglich verlassen, weil eine DNA-Probe abzugeben eine schlechte Idee für sie wäre. Manche haben nach Auskunft der Makler ihren kuwaitischen Pass nur durch Bestechung erlangt und fürchten nun aufzufliegen. Andere haben wohl Angst, weil ihre DNA an für sie eher unvorteilhaften Orten schon gespeichert ist (Baumstieger, Der Emir will´s wissen, SZ 16.09.2016, 1).

Thailand

Touristische Mobilüberwachung

Die staatliche Telekommunikationsbehörde NBTC gab bekannt, dass Thailands Militärjunta künftig TouristInnen elektronisch überwachen will, die sich im Land eine SIM-Karte für ihr Smartphone kaufen. Behördenchef General Takorn Tantasith erklärte, dabei gehe es nicht um die Einschränkung der Rechte der Urlauber, sondern um eine Unterstützung der Polizei, „wenn jemand zu lange im Land bleibt oder auf der Flucht ist“. Die Polizei solle die Sim-Karten nur dann orten dürfen, wenn ein Richter dies zuvor genehmigt.

Bislang können Touristen in Thailand Sim-Karten für ihre Handys kaufen, ohne sich ausweisen zu müssen. Manche Fluggesellschaften verschenken auch Telefonkarten an Passagiere. Nach Thailand reisen jedes Jahr Millionen von TouristInnen, 2016 rund 32 Millionen. Der Tourismus sorgt für ein Zehntel des Bruttoinlandsprodukts.

Seit ihrer Machtergreifung 2014 versucht die Militärjunta, TouristInnen stärker zu kontrollieren. So gab es schon 2014 Pläne, dass jeder Reisende ein sog. Sicherheitsarmband tragen soll, offiziell zu seinem Schutz. Der Polizeichef hatte dies wie folgt begründet: „Wenn Touristen betrunken sind und am Strand einschlafen, können wir sie zurück ins Hotel bringen“. Er verwies auf den Mord an zwei britischen Urlaubern an einem Strand. Diese Pläne waren aber schnell wieder begraben worden.

Anfang 2016 berichteten thailändische Medien, dass persönliche Daten von TouristInnen in einer zentralen Liste gespeichert würden. AusländerInnen, die in Thailand leben und arbeiten, müssen beim Kauf einer Sim-Karte oder beim Abschluss eines Mobilfunkvertrags bereits jetzt eine Kopie ihres Passes vorzeigen. Die thailändische Einwanderungsbehörde verfolgt in jüngerer Zeit einen strengen Kurs unter dem Motto „Bad guys out, good guys in“ (die Schlechten raus, die Guten rein). Wer sich länger im Land aufhält als erlaubt, muss mit einem Aufenthaltsverbot für lange Zeit rechnen (Thailand will Touristen per Sim-Karte überwachen, www.spiegel.de 09.08.2016).

Technik-Nachrichten

Mozilla künftig ohne Akku-Fingerprinting

Mit der Battery Status API können Webseiten den Ladezustand eines Netzgerätes abfragen, worüber Nutzende identifiziert werden können. Eine im Frühjahr 2016 eingeführte Battery Status API wurde wegen Datenschutzbedenken von den EntwicklerInnen des Browsers Firefox aus der kommenden Version 52 des Open-Source-Browsers vollständig entfernt. Die bereits 2012 in Firefox integrierte Funktion wurde vom W3C zunächst als unkritisch eingestuft. Während Browser in der Regel nachfragen, bevor eine Webseite über die Browser-API den Standort eines Nutzenden anfordern darf, kann der Akkuzustand in vielen Browsern in der Standardeinstellung ohne Benutzerintervention abgefragt werden. Theoretisch lässt sich diese Funktion dafür nutzen, um rechenintensive Funktionen einer Webseite wie selbständig abspielenden Videos zu unterbinden, wenn der Nutzende dafür keine Akkukapazitäten mehr zur Verfügung hat.

Mehrere Forschende stellen in einer Studie fest, dass über die API der Ladezustand teilweise auf sechs Nachkommastellen genau sowie exakte Daten zur benötigten Nachladedauer von Notebook, Tablet oder Smartphone übermittelt werden. Mit ein paar Abfragen konnten die Forschenden zudem die Batteriekapazität ermitteln und so einen dauerhaften Identifizierungswert generieren. Diese Möglichkeit wurde auch praktisch genutzt: Forschende der Princeton University in den USA fanden in einer weiteren Studie zwei Skripte, die mit Hilfe der Akku-Werte Nutzende identifizierten, auch wenn diese Cookies gelöscht hatten. Dieses Browser-Fingerprinting kann genutzt werden, um einem Nutzenden neue Cookies zuzuweisen, die ihn dauerhaft kennzeichnen oder ihn auf anderen Websites zu identifizieren. Websites, die die API-Funktion nutzten, um tatsächlich den Akku des Nutzenden zu schonen, entdeckten die Forscher hingegen nicht.

Neben Firefox unterstützen auch Chrome und Chromium-basierte Browser die Battery Status API. Eine Testseite zeigt dem Nutzenden, ob die Funktion aktiviert ist. Wer sich vor solchem Akku-Fingerprinting schützen will, bevor die Firefox-Version 52 im Frühjahr 2017 erscheint, kann die Konfigurations-Seite about:config öffnen und dort die Funktion „dom.battery.enabled" deaktivieren (Kleinz, Datenschutzbedenken: Mozilla entfernt Akku-Fingerprinting aus Firefox. www.heise.de 01.11.2016).

Flexibler Gesundheitssensor ohne eigene Stromversorgung

John Rogers, Forscher an der University of Illinois in Urbana-Champain und Pionier bei der Arbeit mit dehnbarer Elektronik, stellte ein Gerät vor, das auf der Haut zu tragen ist und ohne eigene Batterie Herzschlag und UV-Exposition erfasst. Den nötigen Strom bezieht es über NFC-Funk von einem Mobiltelefon oder Tablet-Computer in der Nähe. Mit diesem Konzept sollen Gesundheitsmessungen billiger, kleiner und leichter werden. Von dem Spezialist für „Epidermis-Elektronik" wurden schon viele Gerätschaften entwickelt, in denen LEDs, winzige Elektronik und Sensoren auf dehnbaren Materialien untergebracht sind. Der neueste Sensor vereint mehrere seiner früheren Innovationen. Er erfasst lichtempfindliche Farben, um Kontakt mit UV-Licht zu registrieren. Er misst darüber hinaus mit Hilfe von vier LEDs, die Lichtstrahlen in unterschiedlichen Farben auf die Haut werfen, den Puls und den Sauerstoffgehalt im Blut. Veränderungen in der Farbe des reflektierten Lichts werden von Photodetektoren erkannt. Der Puls des Trägers wird dann über ein blinkendes Licht angezeigt. Ein Nachteil des batterielosen Design ist, dass der Träger sich nur wenige Zentimeter von Mobiltelefon oder Tablet entfernen darf (Mattke, Pflaster-artiges Gesundheitsmessgerät mit Stromversorgung über NFC, www.heise.de 11.08.2016; Bourzac, Intelligentes Pflaster mit Strom vom Telefon, http://www.heise.de/tr/artikel/Intelligentes-Pflaster-mit-Strom-vom-Telefon-3291509.html).

Rechtsprechung

EGMR

Hausdurchsuchung nach Steuer-CD-Auswertung zulässig

Der Europäische Gerichtshof für Menschenrechte (EGMR) in Straßburg entschied mit Urteil vom 06.10.2016, dass die Nutzung von Steuer-CDs mit illegal beschafften Bankdaten durch Finanzämter nicht gegen die Menschenrechte verstößt, auch wenn auf dieser Grundlage eine Hausdurchsuchung angeordnet wird (33696/11). Geklagt hatte ein deutsches Ehepaar, dessen Wohnung 2008 im Rahmen eines Steuerverfahrens durchsucht worden war. Sie sahen darin eine Verletzung ihres Rechts auf Schutz der Privatsphäre, weil die Durchsuchung erst möglich geworden war, nachdem der Bundesnachrichtendienst (BND) illegal kopierte Bankdaten von der LGT-Treuhand in Liechtenstein gekauft hatte. Das Paar war von der Staatsanwaltschaft Bochum beschuldigt worden, Kapitalerträge in Höhe von 2 Mio. € nicht erklärt und Steuern verkürzt zu haben. Aus Mangel an Beweisen wurde es später freigesprochen.

Das Paar war schon vor dem Bundesverfassungsgericht (BVerfG) im Jahr 2010 mit einer Beschwerde gescheitert (B. v. 09.11.2010, 2 BvR 2101/09, DANA 1/2011, 34 f.). Der EGMR berücksichtigte bei seiner Entscheidung ausdrücklich die Sicht des BVerfG, das die Beschwerde mangels Erfolgsaussicht nicht annahm, wonach es keine absolute Regel gibt, dass illegal erworbene Beweismittel zur Strafverfolgung nicht eingesetzt werden dürfen. Das Paar hätte wissen können, dass die Behörden auch dann darüber nachdenken würden, die Wohnungen zu durchsuchen, wenn sie die Informationen durch Gesetzesbruch erhalten hätten. Außerdem sei die Durchsuchung verhältnismäßig gewesen: Steuerhinterziehung sei ein schweres Vergehen und vor einer generellen Verletzung seiner Rechte sei das Ehepaar geschützt gewesen.

2014 hatte der Verfassungsgerichtshof (VfGH) Rheinland-Pfalz in Koblenz eine Verfassungsbeschwerde eines Kunden der Credit Suisse abgewiesen, dessen Wohnung auch durchsucht worden war. Der VfGH hatte aber betont, es dürfe „auch im Strafverfahren keine Wahrheitsermittlung um jeden Preis geben" (U. v. 24.02.2014, VGH B 26/13, DANA 2/2014, 84). Im Kampf gegen Steuerhinterziehung hat sich das Aufkaufen von Steuer-CDs mittlerweile bewährt: In den vergangenen zehn Jahren erzielte der deutsche Staat Milliardenerlöse mit den Bankdaten mutmaßlicher Steuerbetrüger. Bundesweit haben sich nach Angaben des nordrhein-westfälischen Finanzministeriums seit dem Jahr 2010 rund 120.000 SteuerbetrügerInnen selbst angezeigt (Berger, Gericht billigt Hausdurchsuchungen nach Ankauf einer Steuer-CD, www.sueddeutsche.de 06.10.2016; Leyendecker, Saubere Scheiben, SZ 07.10.2016, 1, 5).

EuGH

Internet-Nutzungsdaten dürfen für Sicherheitszwecke gespeichert werden

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 19.10.2016 entschieden, dass dynamische IP-Adressen, also solche, die sich bei jedem neuen Verbindungsaufbau zum Internet ändern, personenbezogene Daten sind, wenn der Betreiber einer Webseite „über rechtliche Mittel verfügt", Informationen über den Anschlussinhaber hinter der IP-Adresse vom Provider einzuholen (C-582/14). Da es in Deutschland solche rechtlichen Mittel gibt, „die es dem Anbieter von Online-Mediendiensten erlauben, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und anschließend die Strafverfolgung einzuleiten", seien sie datenschutzrechtlich geschützt.

Gemäß § 15 Telemediengesetzes (TMG) dürfen derartige Nutzungsdaten nur für Abrechnungszwecke und um die konkrete, gerade laufende Nutzung eines Onlinedienstes sicherzustellen verarbeitet werden. Die Richter des EuGH sehen in dieser Regelung eine Kollision mit der Europäischen Datenschutzrichtlinie (95/46), die noch bis 2018 gültig ist. Demnach kann es im „berechtigten Interesse" eines Betreibers liegen, „die Aufrechterhaltung der Funktionsfähigkeit" auch über die jeweilige Session des Nutzers hinaus zu gewährleisten. Zu diesem Zweck dürfe ein Betreiber personenbezogene Daten erheben und verarbeiten. Dieses berechtigte Interesse hätten insbesondere die Betreiber der Websites des Bundes, also zum Beispiel die von Ministerien, es sei aber abzuwägen gegen das Interesse oder die Grundrechte der Internetnutzer. Diese Abwägung fehle jedoch im TMG.

Vor mehr als 8 Jahren geklagt hatte der Fraktionsvorsitzende der schleswig-holsteinischen Piratenpartei, Patrick Breyer gegen die Bundesrepublik Deutschland, weil mehrere Bundesministerien und -behörden ungefragt monatelang seine IP-Adresse gespeichert hatten, wenn er ihre Websites aufrief. Breyer betrachtete das als ungerechtfertigten Eingriff in sein Grundrecht auf informationelle Selbstbestimmung und als Verstoß gegen das TMG. Er fürchtet, der Staat könne damit Nutzerprofile anlegen, etwa wenn sie sich auf der Seite des Bundesgesundheitsministeriums über illegale Drogen informieren: „Es muss aufhören, dass Behörden und Konzerne unser Internetnutzungsverhalten verfolgen und aufzeichnen. Das grenzt an Stalking. Was ich lese, schreibe und wonach ich suche, spiegelt meine privatesten und intimsten Interessen, Überzeugungen, Vorlieben und Schwächen wieder und geht niemanden etwas an."

Der EuGH gestand den Website-Betreibern kein Recht zu, ihre Nutzenden zu „verfolgen", sondern stellte klar, dass das TMG nicht länger so ausgelegt werden darf, dass IP-Adressen grundsätzlich nicht gespeichert werden dürfen, um Sicherheitsmaßnahmen für die Webseite durchzuführen. Die Daten könnten bei der Abwehr von Hackerangriffen helfen. Ob das stimmt, wird von Breyer bestritten. Ein Gutachter hatte in der zweiten Instanz des Verfahrens behauptet, die Speicherung von IP-Adressen aus Gründen der IT-Sicherheit sei nicht zwingend erforderlich, es gebe bessere Methoden, Angriffe abzuwehren oder zu verhindern.

Über den konkreten Fall, also ob die deutschen Ministerien ein berechtigtes Interesse an der IP-Adressen-Speicherung haben und ob es die Interessen der Nutzer überwiegt, muss der Bundesgerichtshof (BGH) entscheiden, der den EuGH angerufen hatte. Er findet im EuGH-Urteil aber eine ziemlich unmissverständliche Empfehlung vor (Beuth, Ministerien dürfen IP-Adressen speichern, www.zeit.de 19.10.2016).

EuGH

Passwortschutz bei öffentlichem WLAN-Angebot

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 15.09.2016 zur Störerhaftung entschieden, dass Urheberrechtsinhaber bei geschäftlichen Anbietern von kostenlosem öffentlichen WLAN nicht notwendigerweise einen Anspruch auf Schadensersatz haben, wenn in deren Netz von jemand anderem eine Urheberrechtsverletzung begangen worden ist (C-484/14). Sie können sich aber an eine Behörde oder ein Gericht wenden, wenn es zu einer Urheberrechtsverletzung gekommen ist, wo sie beantragen können, dass der Anbieter des offenen Netzes in Zukunft sein WLAN mit einem Passwort schützen muss. Eine Anordnung zur Sicherung des Anschlusses mit einem Passwort sei geeignet, ein Gleichgewicht zwischen den Rechten am geistigen Eigentum, dem Recht der Anbieter von Internetzugängen auf unternehmerische Freiheit und dem Recht der Nutzer auf Informationsfreiheit zu gewährleisten. Die Nutzenden müssten ihre Identität offenbaren, um das Passwort zu bekommen.

Der EuGH-Generalanwalt Maciej Szpunar kam in wichtigen Teilen zu einem ähnlichen Ergebnis, hatte in seinem Gutachten allerdings weitreichende Auflagen zum Schutz der Hotspots gegen Missbrauch für unzulässig angesehen. Prüfungsmaßstab des Gerichts war die europäische E-Commerce-Richtlinie. Die E-Commerce-Richtlinie, so der EuGH, schließt aber ausdrücklich Maßnahmen aus, die auf eine Überwachung der durch ein Kommunikationsnetz übermittelten Informationen abzielt. Auch eine Maßnahme, die in der vollständigen Abschaltung des Internetanschlusses bestünde, ohne dass die unternehmerische Freiheit des Anbieters weniger beschränkende Maßnahmen in Betracht gezogen würden, wäre nicht geeignet, die einander widerstreitenden Rechte in Einklang zu bringen.

Im aktuellen Fall ging es um den deutschen Piraten-Politiker Tobias McFadden. Sony hatte McFadden bereits 2010 aufgefordert, für ein illegal angebotenes Musikalbum zu zahlen. Über dessen freien WLAN-Hotspot soll ein Album der Gruppe Wir sind Helden zum kostenlosen Download angeboten worden sein. Der Piraten-Politiker hatte in seinen Geschäftsräumen einen offenen Internetzugang eingerichtet. Seitdem prozessierte McFadden mit Unterstützung seiner Partei gegen die Störerhaftung. Das Landgericht in München hatte 2014 das Verfahren ausgesetzt. Der EuGH sollte klären, warum für Konzerne wie die Deutsche Telekom das Providerprivileg

gilt, nicht aber für die Anbieter von offenem WLAN. Beim Providerprivileg geht es darum, dass unter anderem Internetanbieter nicht für die Inhalte von Dritten in ihren Netzen verantwortlich sind.

Wer an der Verletzung eines geschützten Gutes – etwa des Urheberrechts an einer digitalen Datei, aber auch bei Persönlichkeitsverletzungen im Internet – beteiligt ist, ohne selbst Täter zu sein, kann dennoch als sogenannter Störer zur Verantwortung gezogen werden. Immer wieder wegen Urheberrechtsverletzungen im Internet abgemahnt oder auf Schadenersatz verklagt wurden Betreiber öffentlicher Hotspots, über die urheberrechtlich geschützte Dateien getauscht wurden – mit oder ohne Wissen des Betreibers. Da vielfach nur schwer auszumachen ist, wer welche Dateien in Umlauf bringt, wandten sich die Inhaber der Urheberrechte in der Regel an die Hotspot-Betreiber und verwiesen auf die zivilrechtlich begründete Störerhaftung.

In Deutschland hatte es im Juni 2016 eine Änderung des Telemediengesetzes (TMG) gegeben, mit dem die Störerhaftung abgeschafft und Betreiber von WLAN-Hotspots geschützt werden sollten. Künftig sollen damit private Betreiber ihr WLAN für andere öffnen können, ohne wegen Rechtsverletzungen Dritter haftbar gemacht werden zu können. Grüne und Linke hatten dagegen gestimmt, weil sie die Störerhaftung nicht beseitigt sahen und die Entscheidung hierüber lediglich auf die Gerichte abgewälzt würde. Urheberrechtskanzleien hatten ankündigt, auch weiterhin Anbieter von offenem WLAN abmahnen zu wollen. Das deutsche Gesetz sieht vor, dass keine weiteren Zugangshürden zum Netz verpflichtend sein sollen; das sehen, zumindest in konkreten Missbrauchsfällen, die EuGH-Richter anders. Gemäß der EuGH-Entscheidung sollen Betreiber angewiesen werden können, den Zugang per Passwort zu sichern und dabei die Identität der Nutzer zu registrieren.

Das Urteil des EuGH bringt nun für Gewerbetreibe – für private Betreiber ist es nicht übertragbar – die eine kostenlose offene WLAN-Nutzung anbieten, etwas mehr Rechtssicherheit. Im Fall von McFadden wird nun das Landgericht München auf Basis der aktuellen Entscheidung des EuGH entscheiden. Der Kläger McFadden äußerte sich nach der Urteilsverkündung enttäuscht. Das Urteil sei zwar ein Teilerfolg, bleibe aber hinter seinen Erwartungen zurück und lasse nicht auf eine schnelle Verbreitung von WLAN-Hotspots in Europa hoffen. Ein „niederschwelliger Zugang zum Internet“ sei nicht gegeben, wenn man erst um ein „Passwort betteln muss“.

Der Handelsverband Deutschland (HDE) über deren stellvertretenden Hauptgeschäftsführer Stephan Tromp kritisierte: „EU- und Bundespolitik müssen schnell für Rechtssicherheit sorgen. Ansonsten sind die rechtlichen Risiken für Händler, die ihren Kunden freies WLAN anbieten wollen, groß.“ Es sei unrealistisch, allen KundInnen individuelle Passwörter zur Verfügung zu stellen. Der Gesetzgeber müsse zudem Unterlassungsansprüche gegen WLAN-Anbieter eindeutig ausschließen. Ähnlich Markus Luthe, Hauptgeschäftsführer des Hotelverbands Deutschland (IHA): Es werde nun „aller Voraussicht nach bei der gewohnten Prozedur bleiben, dass sich Hotelgäste zuerst registrieren und separate Nutzungsbedingungen anerkennen müssen“. Die Hotellerie habe sich nach dem im März vorgelegten Gutachten des Generalanwalts „eine praxisgerechtere Handhabung des Urheberrechts erhofft“ (Gewerbetreibende haften nicht für offenes WLAN u. Das bedeutet das Urteil zur Störerhaftung für Deutschland, www.spiegel.de 15.09.2016; EuGH, PM Nr. 99/16 15.09.2016, Ein Geschäftsinhaber, der der Öffentlichkeit kostenlos ein WiFi-Netz zur Verfügung stellt, ist für Urheberrechtsverletzungen eines Nutzers nicht verantwortlich).

BVerwG

Kein Informationszugang zu dienstlichen Telefonlisten von Jobcentern

Jobcenter müssen gemäß einem Urteil des Bundesverwaltungsgerichts (BVerwG) vom 20.10.2016 interne Telefonnummern nicht veröffentlichen, da dies die Arbeit in der Behörden behindern würde (7 C 20.15, 7 C 23.15, 7 C 27.15, 7 C 28.15). Das Informationsfreiheitsgesetz des Bundes (IFG) gewährt jeder BürgerIn „einen Anspruch auf Zugang zu amtlichen Informationen“, soweit dadurch nicht die öffentliche Sicherheit oder der Datenschutz gefährdet wird (§ 3 Nr. 2 IFG). Das Gesetz schließt dabei ausdrücklich nicht aus, dass die Behörden auch Namen, Titel oder Telefonnummern von Mitarbeitern angeben. Vier Hartz-IV-Empfänger klagten darauf, die Durchwahl zu der BeamtIn oder SachbearbeiterIn im Amtszimmer zu erfahren. Sie beriefen sich vor Gericht darauf, dass die für sie zuständigen Jobcenter in Köln, Nürnberg und Berlin die Diensttelefonlisten mit den direkten Nummern der Mitarbeiter an sie herausgeben.

Bei den Leipziger Richtern des BVerwG hatten sie mit ihrem Vorstoß jedoch keine Chance: „Einem Anspruch auf Informationszugang zu den dienstlichen Telefonnummern der Bediensteten von Jobcentern können sowohl die Gefährdung der Funktionsfähigkeit der Behörde als auch der Schutz der personenbezogenen Daten der Mitarbeiterinnen und Mitarbeiter entgegenstehen“. Eine Veröffentlichung der Telefonnummern sei nur möglich, wenn „das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt“. Dies sei aber nicht der Fall, da die Daten unter das „Schutzrecht des Grundrechts auf informationelle Selbstbestimmung“ fielen (§ 5 Abs. 1 S. 1 IFG). Das BVerwG erklärte, dass zum Schutzgut der öffentlichen Sicherheit u. a. Individualrechtsgüter wie Gesundheit und Eigentum sowie die Funktionsfähigkeit und die effektive Aufgabenerledigung staatlicher Einrichtungen gehören. Deren Gefährdung liege vor, wenn aufgrund einer auf konkreten Tatsachen beruhenden prognostischen Bewertung mit hinreichender Wahrscheinlichkeit zu erwarten sei, dass das Bekanntwerden der Information das Schutzgut beeinträchtigt. Von diesem rechtlichen Ausgangspunkt aus hatten das Oberverwaltungsgericht (OVG) Münster und der Verwaltungsgerichtshof München jeweils Tatsachen festgestellt, die zu einer solchen Gefährdung führen. Sie bestehe namentlich in nachteiligen Auswirkungen auf die effiziente und zügige Aufgabenerfüllung der Jobcenter, die infolge von direkten Anrufen bei den Bediensteten eintreten können. Das OVG Münster hatte als Vorinstanz entschieden, dass die Weitergabe von

Informationen die Funktionsfähigkeit einer Massenverwaltung wie in einem Jobcenter gefährden würde, wenn viele Leistungsempfänger anrufen, „zu denen mitunter auch Personen mit querulatorischer Neigung zählen“.

Mit dem Grundsatzurteil geht ein jahrelanger Rechtsstreit zu Ende, der für die Bundesagentur für Arbeit (BA) erhebliche Bedeutung hat. Die BA verwaltet mit den Kommunen mehr als 300 Jobcenter. Bei den meisten können die Hartz-IV-EmpfängerInnen ihre BetreuerIn nicht direkt anrufen. Telefonische Anfragen werden über eine einheitliche Hotline und verschiedene Callcenter gebündelt. Die Vermittler sollen so ungestört ihre Akten abarbeiten oder mit den Jobsuchenden an vorher vereinbarten Terminen sprechen können.

Die Kläger und ihre Vertreter reagierten enttäuscht auf das Urteil: Rechtsanwältin Kristina Sosa Noreña meinte, die Richter hätten „die große Chance vergeben, die Jobcenter transparenter für die Bürger zu gestalten“. Sven F., einer der Kläger und Vorsitzender der Erwerbsloseninitiative Braunschweig, bedauerte, dass weiter kein direkter Kontakt mit den Mitarbeitern des Jobcenters möglich sei: „Die eingerichteten Servicenummern werden nun weiter zu einer Vielzahl von Missverständnissen führen, die nicht selten in unnötigen Klagen enden“ (Öchsner, Kein Recht auf Durchwahl, SZ 21.10.2016, 22; Informationszugang zu dienstlichen Telefonlisten von Jobcentern: Revisionen erfolglos, PE BVerwG 20.10.2016).

OVG Rheinland-Pfalz

Racial Profiling: Ermessensfehlgebrauch durch Bundespolizei

Das Oberverwaltungsgericht (OVG) Rheinland-Pfalz in Koblenz stellte mit Urteil vom 21.04.2016 mal wieder fest, dass die Bundespolizei (BPol) bei ihrer Kontrollpraxis in Zügen rechtswidrig agierte (7 A 11108/14). Das OVG meinte aber nicht, dass die zugrundeliegende Regelung diskriminierend und deshalb rechtswidrig sei, sondern, dass hier ermessensfehlerhaft vorgegangen wurde.

Dem Urteil lag folgender Sachverhalt zugrunde: Ein deutsches Ehepaar mit schwarzer Hautfarbe und ihre zwei Kinder saßen in der Regionalbahn von Mainz nach Koblenz. Sie wurden zielgerichtet von zwei Bundespolizisten angesprochen und wegen einer angeblichen Routinekontrolle zur Vorlage von deren Ausweisen aufgefordert. Nach Vorlage der Bundespersonalausweise überprüften sie über Funk, ob diese gestohlen oder gefälscht sind. Davor und danach fand keine weitere Überprüfung anderer Personen statt. Nach der Kontrolle stellen sich die Polizisten an die Tür und stiegen an der übernächsten Station aus. Vor Gericht erklärt die BPol, dass aufgrund ihrer Lageerkenntnisse diese Regionalbahn häufig für die Fortsetzung unerlaubter Einreisen benutzt werde. Als Grund für die Kontrolle ausschließlich dieser Familie erklärten die Polizisten, die Eltern seien gut gekleidet gewesen und hätten mehrere Plastiktüten mit sich geführt. Beides seien Indizien für illegale Grenzübertritte. Mit der Hautfarbe der Personen habe die Kontrolle überhaupt nichts zu tun gehabt. Die Behauptung, dass mehrere Plastiktüten mitgeführt wurden, erwies sich im Rahmen der Beweiserhebung als falsch. Im Bahnwagon befanden sich (weiße) Personen, die sich über das Vorgehen erregten und sich als Zeugen zur Verfügung stellten.

Anders als das Verwaltungsgericht Stuttgart (DANA 2015, 193) und das Amtsgericht Kehl (Vorlagebeschluss an den EuGH) hielt das OVG die Vorschriften des Bundespolizeigesetzes (BPolG) für hinreichend bestimmt und nicht europarechtswidrig. Das OVG meinte auch, in solchen Verfahren gäbe es keine Beweislastumkehr aus Art. 3 GG. Vielmehr müsse der kontrollierte Mensch beweisen, dass hier Racial Profiling vorgekommen ist. Angesichts der näheren Umstände und nach umfangreicher Beweisaufnahme meinte das Gericht allerdings, dass die Hautfarbe zumindest mitentscheidendes Kriterium für die Kontrolle war. Bei dieser Sachlage (nicht nachvollziehbare Auswahlentscheidung) gab es dann aber doch noch eine „kleine Beweislastumkehr“ wegen der fehlenden „Überzeugung des Senats“. Im Urteil finden sich für das Urteilsergebnis nicht relevante, aber interessante Ausführungen zum Schengener-Grenzkodex, der hier nicht verletzt gewesen sein soll.

Eine (unvollständige) Übersicht über anlasslose Kontrollen der Bundespolizei und dazu ergangene Gerichtsentscheidungen findet sich in der Antwort der Bundesregierung auf eine Kleine Anfrage der Fraktion Die Linke im Bundestag. Danach wurden von der BPol 2015 fast drei Mio. anlasslose Personenkontrollen durchgeführt. Von den insgesamt 2.953.844 wurden mehr als 2,6 Mio. im Grenzgebiet durchgeführt, etwas mehr als 248.000 im Inland und rund 69.000 an Flughäfen. Die Linken-Politikerin Ulla Jelpke bemängelte, die Kontrollbefugnisse der BPol „geradezu eine Einladung“, bei anlasslosen Personenkontrollen nach äußerlichen Merkmalen vorzugehen: „Die Bundesregierung deckt diese Praxis, weil sie sich strikt weigert, unmissverständlich klarzustellen, dass die Hautfarbe unter keinen Umständen ein Kriterium für eine Personenkontrolle sein darf. Im Endeffekt werden damit rassistische Kontrollen – racial profiling – geradezu provoziert.“ In der Antwort des Bundesinnenministeriums heißt es hierzu: „Es kann – und das gilt in allen Situationen und für alle Formen des polizeilichen Handelns – auch das äußere Erscheinungsbild einer Person, z. B. die Kleidung, das mitgeführte Gepäck sowie weitere äußere Erscheinungsmerkmale, ein Anknüpfungspunkt an polizeiliche Erkenntnisse und daraus folgende polizeiliche Maßnahmen sein.“ Fahndungsmethoden, die aber „nur und ausschließlich an die äußere Erscheinung von Personen anknüpfen, ohne dass weitere verdichtende Erkenntnisse hinzukommen, sind rechtswidrig und werden daher innerhalb der Bundespolizei weder gelehrt oder vorgegeben noch praktiziert“ (Racial Profiling: Nur Ermessensfehlgebrauch durch Bundespolizei?, ANA-ZAR 3/2016, 28; Bundespolizei führte 2015 drei Millionen „anlasslose Personenkontrollen“ aus, de.nachrichten.yahoo.com 09.04.2016).

OLG München

Facebook-Reproduktion von Foto in Bildzeitung unnötig und deshalb unzulässig

Mit Beschluss vom 17.03.2016 stellte das Oberlandesgericht (OLG) München

fest, dass die Veröffentlichung eines aus Facebook entnommenen Fotos einer Verfasserin eines flüchtlingsfeindlichen Facebook-Kommentars durch „Bild“ und „Bild online“ auf einem „Pranger der Schande“ rechtswidrig war (29 U 368/16). Die Vorinstanz des Landesgerichts (LG) München I hatte die Veröffentlichung für zulässig angesehen.

Mit dem „Pranger der Schande“ lieferte „Bild“ einen gewohnt polternden Beitrag zur Debatte um Facebook-Hasskommentare auf Facebook, indem es rund zwei Dutzend Facebook-Kommentare mit mindestens polemischem, meist offen fremdenfeindlichem Ton zur Flüchtlingskrise abdruckte einschließlich Namen und Profilbildern der Kommentatoren sowie der Aufforderung „Herr Staatsanwalt, übernehmen Sie!“

Eine der angeprangerten Kommentatorinnen beantragte den Erlass einer einstweiligen Verfügung gegen die Abbildung ihres Profilfotos (nicht: ihres Namens oder Kommentars), unterlag jedoch vor dem LG. Sie hatte 2015 auf Facebook geschrieben: „Wie die Tiere und noch schlimmer, alles rennt zum gutgefüllten Futternapf, mal sehen wo Sie hin rennen, wenn unser Napf leer gefressen ist ???“ Das LG meinte, die Veröffentlichung ihres Profilfotos neben dem Kommentar verletze sie weder in ihrem Persönlichkeitsrecht noch – als Fotografin des Profilbildes – in ihrem Urheberrecht. Da die Nutzerin ihr Profilbild ohne Einschränkungen bei Facebook eingestellt habe, sei die weitere Verbreitung durch andere Medien im Internet nach der Rechtsprechung des EuGH schon keine weitere öffentliche Wiedergabe. Die Schranke des § 48 Urheberrechtsgesetz (UrhG) für die Wiedergabe öffentlicher Reden durch Medien sei auf die Verbreitung von Facebook-Posts samt Profilbild analog anzuwenden. Ferner sei die Veröffentlichung des Screenshots sowohl vom Zitatrecht nach § 51 UrhG als auch von der Schranke für Tagesereignisse nach § 50 UrhG gedeckt.

Damit entsprach das LG auch der herrschenden veröffentlichten Meinung von JuristInnen, die darauf abstellte, dass die Beiträge in einer für jeden Facebook-Nutzenden einsehbaren Form abgegeben worden waren und die Kommentatoren durch ihren Abdruck auch nicht in ihrer Privat- oder gar Intimsphäre berührt wurden. Auch der Bezug zur aktuellen gesellschaftlichen Debatte streite im Rahmen der Abwägung nach § 23 Kunsturhebergesetz (KUG) für ein Veröffentlichungsrecht der Medien.

Das OLG vertrat jedoch eine andere Auffassung. Es verzichtete in der mündlichen Verhandlung auf eine Auseinandersetzung mit deren urheberrechtlichen Begründungen und argumentierte allein mit dem Persönlichkeitsrecht der Frau, das verletzt worden sei: Zwar sei ein klarer zeitgeschichtlicher Bezug der Berichterstattung gegeben. Allerdings hätte die Zeitung das Foto der Frau ebenso gut weglassen bzw. in verpixelter Form zeigen können. Die unverpixelte Darstellung schaffe keinerlei Mehrwert für die Leser, stelle aber einen intensiveren Eingriff in die Rechte der Betroffenen dar. Die Veröffentlichung von Fotos im Internet beinhalte nicht automatisch ein Einverständnis in jedwede weitere Verbreitung.

Der Bild vertretende Anwalt Ulrich Amelung kritisierte die OLG-Entscheidung: „Es ist ein eherner Grundsatz des Presserechts, dass die Entscheidung darüber, welchen Mehrwert ein Bild liefert, allein dem Medium überlassen bleibt.“ Die Frage danach, ob der Artikel ohne das Foto genauso aussagekräftig gewesen wäre wie mit, hätte das Gericht nicht in die Abwägung nach § 23 KUG einfließen lassen dürfen. „Irritierenderweise hat hier ausgerechnet der für Urheberrecht zuständige Senat des OLG entschieden, aber das mit einer rein presserechtlichen Begründung, die so nicht haltbar ist.“ Da Rechtsmittel gegen die Entscheidung im einstweiligen Rechtsschutzverfahren nicht statthaft sind, werde man nun das Hauptsacheverfahren anstreben (Baron van Lijnden, „Pranger der Schande“ doch rechtswidrig, www.lto.de 21.03.2016; Wurzberger, Facebook-Foto in „Bild“ rechtswidrig, CuA 9/2016, 25).

LG Köln

BMW-Hersteller-Daten bei Straßenverkehrsunfall-Urteil hinzugezogen

Nach einem tödlichen Unfall mit einem BMW des Car-Sharing-Anbieters Drive Now wurde der 27jährige Fahrer, ein BWL-Student, vom Landgericht (LG) Köln am 23.05.2016 zu einer Haftstrafe von 33 Monaten verurteilt (113 KLs 34/15). Im Prozess spielten Daten aus dem Fahrzeug eine wichtige Rolle. BMW hatte detaillierte Daten der Unfallfahrt vorgelegt. Der 27-Jährige hatte im Sommer 2015 den Unfall mit einem anderen Fahrzeug verursacht, bei dem ein an der Ampel wartender 26-jähriger Fahrradfahrer getötet wurde. Anhand der von BMW zur Verfügung gestellten Daten konnte dem Fahrer nachgewiesen werden, dass er bis zum Unfall im Stadtgebiet mit stark überhöhter Geschwindigkeit – stellenweise über 100 km/h – unterwegs war. Das LG-Urteil befasste sich nicht mit der Frage, ob die Datenerhebung, die der Sachverständige zu Grunde legte, rechtmäßig war. Selbst bei einer Unzulässigkeit wäre aber nach etablierter Rechtsprechung im vorliegenden Fall kein Beweisverwertungsverbot anzunehmen gewesen.

Drive Now, eine Tochtergesellschaft von BMW und Sixt, erklärte dazu, dass das Unternehmen keine Fahrprofile von Kunden anlege. Zu Abrechnungszwecken erfasse das Unternehmen nur Start und Ziel sowie die Dauer der Fahrt: „Diese Daten benötigen wir für die Rechnungserstellung und speichern sie im Rahmen der gesetzlichen Aufbewahrungsvorschriften“. Das steht so auch in den AGB des Anbieters, die Nutzer des Dienstes zur Kenntnis nehmen müssen.

Tatsächlich stammen die vor Gericht ausgewerteten Daten direkt vom Fahrzeughersteller. BMW betonte, dass in normalen BMWs diese Daten nicht gespeichert werden: „Die BMW Group erhebt und speichert keine Bewegungsprofile ihrer Kunden“. Es handele sich um besondere Module, die ausschließlich in den Car-Sharing-Modellen des Herstellers eingebaut seien. Das Car-Sharing-Modul (CSM) speichere während der Fahrt bestimmte Daten zum Fahrzeugzustand und -betrieb.

Diese Daten werden, so eine BMW-Sprecherin, „ausschließlich von der BMW Group und nur im Einzelfall zu konkreten Supportzwecken bei Kundenrückfragen, Beschwerden oder technischen Problemen abgerufen“. Die Daten für das Verfahren in Köln seien „nach behördlicher Aufforderung“ aus dem CSM abgerufen und aufgrund einer

staatsanwaltlichen und gerichtlichen Anforderung an das LG Köln herausgegeben worden. Es bestehe keine Verknüpfung mit den Vertragsdaten des Kunden des Car-Sharing-Anbieters, diese sei erst vor Gericht erfolgt (Briegleb, Car-Sharing-Unfall: Aufregung um angebliche Datenprofile in BMWs, www.heise.de 22.07.2016).

AG Bad Hersfeld

Vater muss bei Kindern Messengerdienst entfernen

Gemäß einem Beschluss des Amtsgerichts (AG) Bad Hersfeld vom 22.07.2016 muss ein Vater, nachdem ihm bekannt wurde, dass seine minderjährigen Töchter über einen längeren Zeitraum Opfer von Messenger-Kommunikation mit sexualisierten Inhalten („Sex-Texting" oder „Sexting") waren, dies künftig zu verhindern suchen und hierfür u. a. WhatsApp und vergleichbare Programme von den Smartphones der Töchter zu entfernen (Az.: F 361/16 EASO). Zudem wurde er verpflichtet, mit den Minderjährigen monatlich ein Gespräch über die Nutzung zu führen und die Smartphones alle drei Monate zu prüfen, welche Apps darauf installiert sind und ob es darauf Ungereimtheiten gibt.

Die Eltern der 2000 und 2005 geborenen Mädchen hatten sich im Jahre 2006 getrennt und sind geschieden. Die Kinder blieben nach der Trennung zunächst im Haushalt der Kindesmutter, zogen aber später zu ihrem Vater. Beide besaßen Smartphones, auf denen neben anderen Programmen auch jeweils die Messenger-App WhatsApp installiert war. Im Mai 2016 erstattete die ältere Tochter Anzeige wegen des Verdachts der sexuellen Belästigung gegen einen ehemaligen Schulfreund ihres Vaters. Die Kindesmutter beantragte, dass die elterliche Sorge für beide Töchter auf sie übertragen wird. Diesen Antrag zog sie später zurück. Doch erteilte das Gericht dem Vater die Auflagen nach § 1666 Bürgerliches Gesetzbuch (BGB). Dieser regelt gerichtliche Maßnahmen bei Gefährdung des Kindeswohls. Nach Ansicht des Gerichts sind diese notwendig, um eine früher aufgetretene und weiterhin gegebene Gefahr abzuwehren.

Das Gericht stellte fest, dass die über zwölf Monate andauernde, vehemente und ausdauernde Kommunikation über WhatsApp die Schwestern stark ergriffen und ihr Wohlbefinden sichtlich negativ beeinträchtigt hat. WhatsApp stelle für Kinder und Jugendliche unter 16 Jahren „grundsätzlich eine Gefahr für ihre Privatsphäre und ihre Entwicklung dar". Dies gelte zumindest dann, wenn die Kinder vor jener Nutzung nicht einen „ausgeprägten verantwortungsvollen Umgang mit den Funktionen und den Risiken aufgezeigt bekommen haben und wenn sie nicht bereits eine besondere geistige Reife und vorausschauende Sicht im Hinblick auf die Nutzung aufweisen".

Das Gericht wies darauf hin, dass „Smart-Geräte aufgrund ihrer vielfältigen technischen Möglichkeiten und ihrer vernetzten Anbindung nicht als einfaches elektronisches Spielzeug angesehen werden können, welches den Kindern schlicht und ohne jegliche Überwachung ausgehändigt werden könnte". Besonnene vernünftige Eltern, die ihren Kindern solche Geräte überlassen, müssten laufend sicherzustellen, dass diese sich mit den möglichen Risiken und Gefahren an dem Gerät auskennen und darauf jeweils adäquat reagieren können. Zusätzlich biete sich insbesondere bei der jüngeren Tochter eine digitale Kindersicherung an. Der Vater muss gegenüber dem Familiengericht nachweisen, dass er den Auflagen nachgekommen ist (Heidrich, Vater muss WhatsApp von den Mobilgeräten seiner Kinder entfernen, www.heise.de 11.08.2016).

AG Hannover

Retortenbabys haben Anspruch auf Namen von Samenspender

Gemäß einem Urteil des Amtsgerichts (AG) Hannover vom 17.10.2016 darf eine Reproduktionsklinik einer Frau, die wissen möchte, wer ihr Erzeuger ist, den Namen nicht länger verheimlichen (432 C 7640/15). Die 21-Jährige war als Retortenbaby zur Welt gekommen und hatte die Klinik darauf verklagt, ihr den Namen des Mannes zu nennen, mit dessen Samenspende sie einst gezeugt worden war. Ihre Mutter hatte sich künstlich befruchten lassen, da ihr Ehemann zeugungsunfähig war. Auf Anfrage hatte sich die Klinik zunächst geweigert, den Namen des Samenspenders zu nennen, obwohl die Rechtsprechung in dieser Frage inzwischen eindeutig ist. Bereits 2015 hatte der Bundesgerichtshof (BGH) geurteilt, dass Kinder ein Recht darauf haben, den Namen ihres biologischen Vaters zu erfahren. In der Praxis verweigern jedoch immer noch viele Kliniken die Auskunft.

Der Klinik-Anwalt begründete die Verweigerungshaltung: „Der Samenspender war davon ausgegangen, dass sein Name geheim gehalten wird." Sollte er nach dem Verlust seiner Anonymität Schadensersatzansprüche gegenüber der Klinik stellen, z. B. weil seine biologische Tochter Unterhalts- und Erbansprüche geltend macht, brauche man Rechtssicherheit. Die Furcht vor Unterhaltsansprüchen ist aber nach Ansicht des Vereins Spenderkinder unbegründet: „Keinem uns bekannten Spenderkind geht es um finanzielle Forderungen gegenüber dem Spender." Der Verein fordert sogar eine rechtliche Klärung, dass Erbansprüche und Unterhaltsforderungen ausgeschlossen sind. Jeder Mensch habe jedoch ein Recht, seine genetische Herkunft zu erfahren.

Dem BGH zufolge können Informationen über den biologischen Vater „für die Entfaltung der Persönlichkeit von elementarer Bedeutung sein". Für den Samenspender müsse die Auskunft zwar zumutbar sein. „Nicht maßgeblich" seien dabei aber „seine wirtschaftlichen Interessen". Im Bundesgesundheitsministerium wird an den institutionellen und organisatorischen Voraussetzungen gearbeitet, damit jedes Kind sein Recht auf Herkunftskenntnis umsetzen kann. Dazu soll ein zentrales Spenderregister eingeführt werden (Der Name zum Samen, SZ 18.10.2016, 10).

Buchbesprechungen



Wedde, Peter
EU-Datenschutz-Grundverordnung Kurzkommentar mit Synopse BDSG/ EU-DSGVO
Bund-Verlag Frankfurt/Main 2016, 346 S., ISBN 978-3-7663-6589-7, 39.90 €

(tw) Viele der nach Bekanntwerden der DSGVO erfolgten kurzfristigen Veröffentlichungen verfolgen noch nicht das Ziel und haben auch nicht den Anspruch, inhaltlich in die Tiefe zu gehen. Vielmehr zielen sie darauf ab, einen Überblick zu verschaffen und eine erste Orientierung über das zu vermitteln, was sich ändert, was gleich bleibt und welche nächsten Schritte unternommen werden müssen.

Zu dieser Kategorie gehört auch die Dokumentation von Peter Wedde. Dessen Zielgruppe ist nicht der Gesetzgeber (so Kühling/Martini u.a., DANA 3/2016, 159; Roßnagel, s. u.), auch nicht der Unternehmensjurist (so Laue/Nink/Kremer, Härting, DANA 3/2016, 158 f.), sondern der allgemein Interessierte bzw. angesichts des üblichen Publikums des Bund-Verlags die Arbeitnehmerseite. Das Buch teilt sich in 4 Teile: einen allgemeinen Überblick, den Abdruck der Erwägungsgründe, den Abdruck der DSGVO mit Verweisen zu den Erwägungsgründen sowie eine Synopse, in der auf Grundlage des bisherigen BDSG Verweise zur DSGVO vorgenommen werden.

Die Sammlung von Wedde erfüllt damit die Funktion eines Referenzsystems, mit dem bei der Suche nach den neuen gültigen Regeln vom BDSG über die DSGVO bis hin zu den Erwägungsgründen die offiziellen Informationen gut und leicht erschlossen sind. Insofern ist das handliche Werk äußerst hilfreich. Für die Beantwortung offener oder streitiger Fragen liefert sie keine eigenen Positionen.



Albrecht, Jan Philipp/Jotzo, Florian
Das neue Datenschutzrecht der EU
Nomos-Verlag Baden-Baden, 2016, ISBN 978-3-8487-2804-6, 339 S., 48,00 €

(tw) Mit der Veröffentlichung des endgültigen Textes der Europäischen Datenschutz-Grundverordnung (DSGVO) wurde ein Rennen von Verlagen und Wissenschaftlern ausgelöst, wer als erster mit seiner Publikation und Meinung hierzu auf dem Markt ist. Manches, was dabei publiziert wurde, wird nicht von längerer Gültigkeit sein. Nicht zu den allerersten, dafür aber garantiert zu den längerlebigen Publikationen gehört das Buch von Albrecht/Jotzo, weil es Einsichten über die Hintergründe und den Entstehungsprozess des neuen EU-Datenschutzrechts gewährt, was andere Schriften nicht vorweisen können. Dies erklärt sich damit, dass einer der Autoren, Jan Philipp Albrecht, persönlich nicht nur an der Entstehung dieses Rechts beteiligt war, sondern als Berichterstatter des Europäischen Parlaments für die DSGVO, gemeinsam mit der EU-Kommissarin Vivian Reding, wohl den wichtigsten Part überhaupt im Gesetzgebungsverfahren spielte.

Das Werk bezieht sich auf das gesamte neue EU-Datenschutzrecht, doch liegt dessen Schwergewicht eindeutig bei der DSGVO. Es beschreibt auf über 100 Seiten gedrängt die Geschichte der Gesetzgebung, die rechtlichen und politischen Erwägungen von Kommission, Parlament und Rat und, wer sich mit was, wie und weshalb am Ende beim Trilog durchgesetzt hat. Dabei wird mit der kenntnisreichen Innenansicht auch in Bezug auf die vielen beantworteten und auch unbeantworteten rechtlichen Einzelfragen dargelegt, welche nationalen und ökonomischen Hintergründe eine Rolle spielten. Es wird erkennbar, dass die DSGVO, so wie sie nun in Kraft getreten ist, ohne die Enthüllungen von Edward Snowden – sowohl im Hinblick auf den Inhalt wie auch auf den Einigungszwang – nicht zustande gekommen wäre.

Albrecht hat sich während des Gesetzgebungsverfahrens als sehr engagierter Vertreter eines stark grundrechtsorientierten Datenschutzes profiliert. Diese Linie behält das Buch bei, jedoch mit einer hinsichtlich der beschriebenen Normen und deren Genese erfrischenden Objektivität. Es beschreibt, wie europäisches Recht generell auszulegen ist und wie die DSGVO im Konflikt zwischen Harmonisierung und nationalen Rechtskulturen unter Wahrung von Subsidiarität und Verhältnismäßigkeit einzuordnen ist. Zweifellos lässt sich aus Datenschutzsicht beklagen, dass viele Öffnungsklauseln der DSGVO für einen einheitlichen Datenschutz nicht förderlich sind. Es wird aber nachvollziehbar dargelegt, dass mehr an einheitlichem Datenschutz nicht möglich war. Damit zeichnet sich ab, anders als dies noch bei der Richtlinie Anfang der 90er Jahre war, dass mit der DSGVO ein realer Fortschritt für den digitalen Grundrechtsschutz – nicht nur in der EU – erreicht wird. Albrecht/Jotzo lassen erkennen, dass dem Text der DSGVO keine billigen Kompromisse zugrunde liegen, sondern dass dieser nach langer Reflexion und kontroverser Diskussion einer hohen Rationalität verpflichtet ist.

Wer nun zu allen brennenden Fragen zur DSGVO von dem Buch eine Antwort erwartet, der muss enttäuscht werden. Dies kann ein derart konzentriertes frühes Werk nicht leisten. Wohl aber gibt es viele Hinweise beim Austragen

künftiger Auslegungskontroversen. So ist aufschlussreich, dass dem Gesetzgeber bewusst war, dass die als Betroffenenrecht ausgestaltete Regelung zu Big Data und Profiling in Art. 20 eine Notlösung bleiben musste, mit der künftige Präzisierungen nicht verhindert, sondern gefördert werden sollte. Ähnliches gilt für die weiten normöffnenden Ausnahmekataloge zu den Betroffenenrechten in Art. 23, die Regelung zum Beschäftigtendatenschutz (Art. 88) oder die zum Verhältnis zur Meinungs- und Informationsfreiheit (Art. 85). Aufschlussreich ist auch, dass bei der Ausgestaltung der Sanktionen offenbar das Kartellrecht Pate stand – eine Absage an die bisherige deutsche Sanktionenpraxis, die sich eher an Verstößen gegen die Straßenverkehrsordnung orientiert. Spannend sind weiterhin die Erwägungen zu den Zusammenarbeitsregelungen der Aufsichtsbehörde, mit denen Neuland betreten wurde. Bewähren sie sich, so können sie Vorbild für die europäische administrative Kooperation in anderen Bereichen werden.

Als Rechtsquelle gut geeignet und leicht zu handhaben ist die abgedruckte Synopse mit dem Text der DSGVO und der Europäischen Datenschutzrichtlinie sowie den aktuell dazu gehörenden Erwägungsgründen, über die sich nicht nur die europäische Rechtsentwicklung, sondern auch die Normkonkretisierung nachvollziehen lässt, zumal Erwägungsgründe im europäischen Recht einen höheren Verbindlichkeitsgrad haben als etwa im nationalen Recht Gesetzesbegründungen. Der Quellencharakter des Werks wird dadurch verstärkt, dass die Positionen von Kommission, Rat und Parlament in der Vorphase der Gesetzgebung über das „Gesamtkonzept für den Datenschutz“ abgedruckt sind und in den Fußnoten Bezüge zu vielen weiteren europäischen Vorgängen hergestellt werden. Das Stichwortverzeichnis und ein aktuelles, selektives Literaturverzeichnis erschließt Textpassagen in dem Buch und zu in den verweisenden Fußnoten aufgeführten weiterführenden Texten.

Das Werk ist angesichts des Umstands, dass die historische Auslegung beim EU-Recht ebenso wie generell von hoher Bedeutung ist, bei der Beantwortung vieler offenen Fragen zur DSGVO für Wissenschaft wie für die Praxis unersetzlich. Es ist aber in seiner Kürze und Prägnanz auch für interessierte Datenschützer und Juristen ein geeigneter Einstieg in das EU-Datenschutzrecht. Durch seine klare, einfach zu verstehende und dennoch die Komplexität der Sachverhalte darstellende Sprache ist es nicht nur den Juristen, sondern auch Vertretern anderer Disziplinen zugänglich. Wer es nicht schon wusste, erkennt spätestens nach der Lektüre des Buchs: Mit dem Inkrafttreten der DSGVO fängt die Arbeit für alle Beteiligten – nationale wie europäische Gesetzgeber, Aufsichtsbehörden, generell Datenschützer, Wissenschaft, Unternehmen und Behörden – erst richtig an; das Buch ist für diese Arbeit äußerst nützlich.



Roßnagel, Alexander (Hrsg.)
Europäische Datenschutz-Grundverordnung
Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts
Nomos Baden-Baden 2017, ISBN 978-3-8487-3074-2, 342 S., 48,00 €

(tw) Ähnlich wie die Arbeit von Kühling/Martini u. a. (DANA 3/2016, 159) nimmt sich die von Roßnagel herausgegebene Kollektivarbeit der – die Gesetzgeber und die Wissenschaft interessierende – Schnittstelle zwischen deutschem und europäischem Datenschutzrecht an: Welche Vorschriften des deutschen Datenschutzrechts werden von der Datenschutz-Grundverordnung (DSGVO) verdrängt und welche bleiben auch nach der direkten Anwendbarkeit des DSGVO vom 25.05.2018 an anwendbar. Dabei behandelt sie zunächst die grundsätzliche Frage des Verhältnisses von nationalem und europäischem Recht. Danach widmet sie sich der Frage, inwieweit konkret der DSGVO Vorrang einzuräumen ist und welche Spielräume dem nationalen Gesetzgeber bleiben, wobei dies zum einen gemäß der Struktur des DSGVO und dann bezogen auf einzelne Bereiche der Datenverarbeitung abgehandelt wird. Bei der Behandlung der einzelnen Artikel der DSGVO verharren die AutorInnen nicht bei der Frage des Anwendungsvorrangs, sondern steigen in die zentralen materiell-rechtlichen Fragen ein.

Die allgemeine einführende Darstellung kommt zu dem Ergebnis, dass die Ansprüche der DSGVO, nämlich das Recht zu vereinheitlichen, die Praxis anzugleichen und das Recht zu modernisieren, nicht oder nur begrenzt erreicht werden. Die Rechtsprechung des Bundesverfassungsgerichts mit seiner Ausdifferenzierung des Datenschutzes wird sodann mit der Europäischen Grundrechte-Charta, der Rechtsprechung des EuGH und den DSGVO-Regelungen abgeglichen. Dabei erweist sich eine weitgehende Kongruenz und dass, entgegen mancher Befürchtung, die bisherigen Rechtsschutzmöglichkeiten sich ändern, aber im Wesentlichen nicht verloren gehen. Die Einführung des Marktortprinzips wird als eine wichtige Errungenschaft der DSGVO hervorgehoben. In Bezug auf die Erlaubnistatbestände wird registriert, dass diese sehr allgemeiner Natur sind und durch Öffnungsklauseln – aber nur in bestimmten Bereichen – nationalen Gestaltungsspielraum lassen. Positiv bewertet wird, dass im Rahmen der Datenschutz-Folgenabschätzung eine vertiefte und komplexere Prüfung erfolgen muss, als dies bisher vom Recht gefordert war. Es irritiert, dass neben den Regelungen zur Datensicherheit weiterhin ein Anwendungsbereich für § 9 BDSG mit seiner Anlage gesehen wird. Berechtigt ist die Kritik, dass Hersteller von Verarbeitungssystemen nicht bzw. nur ganz indirekt in die Regulierung mit einbezogen wurden. Die Neuorganisation des Aufsichtsbereichs und die – komplexen – Kooperationsregeln werden im Ergebnis positiv kommentiert.

In einem umfangreichen Kapitel befassen sich die AutorInnen mit der Frage, welche Auswirkungen die DSGVO auf besondere Bereiche der Datenverarbeitung haben. Dabei stehen folgende zentrale Anwendungen im Fokus: der öffentliche Bereich, der im nationalen Recht weitgehend unverändert bleiben kann, der nur allgemein durch die DSGVO

vorgegebene Beschäftigtendatenschutz, der Sektor von Forschung, Wissenschaft, Statistik und Archiven sowie die offenen Flanken der DSGVO durch die Medienprivilegierung und die Informationsfreiheit. Weitere behandelte Einzelbereiche sind die Telekommunikation, die Telemedien, die Verarbeitung von Gesundheitsdaten und Berufsgeheimnissen sowie der Bereich der sozialen Sicherheit.

Das Werk entstand innerhalb der vom Herausgeber koordinierten Projektgruppe verfassungsverträgliche Technikgestaltung (provet), die sich im Rahmen vieler sich mit Datenschutzfragen befassender Einzelprojekte in spezifischen Bereichen sowohl des öffentlichen wie auch des nicht-öffentlichen Datenschutzes mit der Geltung der DSGVO befassen muss. Auch die parallel verabschiedete Datenschutzrichtlinie für Polizei und Justiz wird dargestellt. Zu der Projektgruppe gehören neben dem Herausgeber Charlotte Barlag, Christian L. Geminn, Johanna Hofmann, Carolin Hohmann, Dominik Hoidn, Silke Jandt, Paul C. Johannes, Natalie Maier, Kevin Marschall, Maxi Nebel, Verena Ossoinig, Fabian Schaller und Robert Weinhold. Deren kritische Ausführungen zielen nicht darauf ab, die Daseinsberechtigung der DSGVO zu negieren oder deren Anwendung zu obstruieren, sondern die Finger in Wunden zu legen, um die nationale Gesetzgebung, die Wissenschaft und perspektivisch die Rechtsprechung zur Klärung zu veranlassen. Das Werk kommt in vielen Bereichen zum Ergebnis, dass nationales Datenschutzrecht neben der DSGVO anwendbar bleibt. Diese weitherzigen Ergebnisse sind insofern verblüffend, dass eingangs beklagt wurde, dass das Harmonisierungsziel mit der DSVGO verpasst worden sei. Hier dürfte der EuGH in zu entscheidenden Einzelfällen sicherlich anderer Meinung sein.

Prof. Dr. Gerrit Manssen (Hrsg.),
Telekommunikations- und Multimediarecht
Ergänzungslieferung vom September 2016, ISBN 978-3-503-16991-7, ESV-Verlag

(wh) Im Gesetzestext werden neben anderen Änderungen zwar bereits die aus Datenschutzsicht wesentlichen Änderungen des TKG durch Art. 2 des „Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (vulgo: Gesetz zur Einführung der Vorratsdatenspeicherung) aufgenommen. In der Kommentierung finden sich diese Änderungen allerdings noch nicht wieder. Kommentiert werden neu die §§ 21, 22 und 25 TKG, ergänzt wird die Kommentierung des § 20 TKG. Daher ist diese Ergänzungslieferung für die am Datenschutz interessierten InhaberInnen der Loseblattsammlung zwar aus Gründen der Vollständigkeit erforderlich, inhaltlich aber nicht von Belang.

Dr. Philip Laue, Dr. Judith Nink, Sascha Kremer,
Das neue Datenschutzrecht in der betrieblichen Praxis
ISBN 978-3-8487-2377-5, 1. Auflage 2016, Nomos, 326 S., 48 €

(wh) Auch wenn es der Titel nur indirekt widerspiegelt, beim dem Werk handelt es sich um ein Praxishandbuch zur Anwendung der EU-Datenschutz-Grundverordnung (DSGVO). Die AutorInnen haben mit der Erstellung dieses Praxishandbuchs bereits während des Gesetzgebungsverfahrens begonnen. Der kompakte Umfang (326 Seiten) ist u.a. darin begründet, dass es derzeit noch keinerlei Erfahrungen mit der Umsetzung der Vorschriften in der Praxis gibt. So schreiben die AutorInnen selbst überraschend offen: „Wo mangels Parallelen zur bisherigen Rechtslage nicht auf gesicherte Erkenntnisse oder Hinweise aus dem Gesetzgebungsverfahren zurückgegriffen werden konnte, bedurfte es daher an der einen oder anderen Stelle auch des Blicks in die datenschutzrechtliche Glaskugel.“ In Bezug auf die EuGH-Entscheidung zur der Frage, ob IP-Adressen personenbezogene Daten sind – diese Entscheidung stand beim Redaktionsschluss des Werkes im Juli 2016 noch aus – wurde kein „Blick in die Glaskugel gewagt“, sondern nur ein entsprechender Hinweis auf dieses Verfahren gegeben.

Es werden alle im betrieblichen Datenschutz relevanten Themengebiete in übersichtlich strukturierter Form praxisbezogen behandelt. Dort wo es sinnvoll ist, wurden den neuen Rechtsgrundlagen die Rechtsgrundlagen aus dem Bundesdatenschutz gegenüber gestellt. Ein umfangreiches Literaturverzeichnis und ein ausführliches Stichwortverzeichnis runden das empfehlenswerte und auch preisliche angemessene Werk ab.



Lanier, Jaron
Wem gehört die Zukunft ? – Du bist nicht der Kunde der Internetkonzerne. Du bist ihr Produkt
Hoffmann und Campe, Hamburg 2013, ISBN 978 3455550 03180, 480 S.
(Englisch: Who owns the Future? Simon&Schuster, New York 2013)

Die Computerexperten in Silicon Valley glauben überwiegend, sie würden die Welt in eine phantastische Zukunft führen. Lanier glaubt, dass vielmehr die Gefahr besteht, dass der Mensch keine Rolle mehr spielt. Das Internet ist kein Instrument der Freiheit, wie es viele lange geglaubt haben. Vielmehr werden die Netze und die Kommunikation darin von wenigen großen Konzernen kontrolliert und gesteuert.

Er kritisiert die Sirenenserver in Anspielung an die lieblichen Sirenen in Homers Odyssee, die alle Menschen anlocken und dann versklaven. Darunter fasst er alle Internetanwendungen, die in großem Umfang meist kostenlos riesige Datenmengen sammeln. Indem sie die immer größeren Datenmengen („Big Data“) immer geschickter auswerten, sind sie in der Lage, die Geschäfte immer optimaler zu gestalten und kleine Konkurrenten auszuschalten. Gleichzeitig gewinnen sie so immer mehr Macht und beginnen zunehmend damit die Nutzer zu manipulieren. Da die Daten/Profile, die die Nutzer eingegeben haben, an den Sirenenserver gebunden sind, ist der Nutzer immer mehr gefesselt, da er bei der Kündigung des Servers auch seine Kontakte verliert. Auch verlagern sich wichtige Debatten, Informationskanäle usw. in private Plattformen wie Facebook. Man kann dann Facebook nicht

mehr meiden, ohne sich selbst von den Informationen auszuschließen.

Sirenenserver sind also Facebook, Google, Amazon und Apple Store, aber auch Versicherungen, Krankenkassen, Banken, Geheimdienste (in den USA auch die beiden großen Parteien) sowie alle anderen Firmen und Einrichtungen, die in großem Stil Daten über ihre Kunden bzw. Nutzer sammeln. Die Ökonomie der Netze bevorteilt systematisch die Großen gegenüber den Kleinen, da sie mehr Daten haben und optimalere Verknüpfungen erstellen können. Alle Risiken werden ausgelagert durch Erklärungen des Haftungsausschlusses, die niemand liest. Ergebnis ist ein „Starsystem“, wie man es klassischerweise im Sport kennt. Für die Masse ist es Hobby, nur sehr wenige verdienen etwas und ganz wenige werden reich. Es gibt also nicht viele kleine Firmen; sondern bei jeder Anwendung bleibt am Schluss von vielen Start-Ups nur einer übrig: „The Winner takes All“. Alle anderen Millionen App-Entwickler bleiben auf der Strecke.

Das Ergebnis wird sein, dass die Produkte zunehmend kostenlos sind, also nichts mehr damit zu verdienen ist. Beispiel dafür ist heute schon die Musikindustrie, wo die meisten Künstler an ihren Produkten nichts mehr verdienen können, da alles kostenlos im Internet kopiert wird. Es bleiben ihnen nur die Live-Auftritte. Deswegen ist der Musikmarkt weltweit zusammengebrochen. Die nächste Berufsgruppe, die durch das Internet in ihrer Existenz bedroht ist, sind die Journalisten. Das gleiche wird mit zahlreichen anderen Märkten geschehen, wenn die Systeme, Server und Roboter immer besser werden. Am Schluss wird die Masse verarmen und die Ökonomie wird immer mehr schrumpfen.

Eine prosperierende Wirtschaft ist nur möglich, wenn die Größe der Betriebe sich wie eine Glockenkurve verteilt – also mit einem wohlhabenden Mittelstand. Im Gegensatz dazu konzentriert sich bei der „Starsystem“-Kurve das gesamte Vermögen bei den extrem großen Konzernen. Ein Starsystem gefährdet auch die Demokratie. Autoritäre Systeme wie in China werden selbst zu Sirenenservern, die alle Daten über die Bürger sammeln, auswerten und die Bürger*innen manipulieren. In den Demokratien gibt es einen Wettstreit zwischen den Sirenenservern der Wirtschaft und Finanzmärkte, die dann die Demokratie durch Geld und Manipulation aushebeln. Alternativ entwickelt sich die Regierung bzw. die Parteien ebenfalls zu Sirenenservern, die dann aber nur noch Elitenprojekte sind. Deswegen kommt Lanier zu dem Schluss: „Wenn man die Demokratie erhalten will, ... (muss) die Mittelschicht zusammengenommen mehr Geld haben ... als die Eliten. Die Glockenkurve muss die Starprinzip-Kurve übertrumpfen.“

Im Alten Kapitalismus gab es viele Dämme, die dafür gesorgt haben, dass der Mittelstand geschützt wurde und die Glockenkurve erhalten blieb: Sozialgesetze, Gewerkschaften, progressive Steuern und viele Regulierungen. Diese Dämme sind durch das Internet (und die damit sich verbreitende neoliberale Philosophie) immer mehr eingerissen worden. Auch die Verlagerung von Kommunikation auf private Plattformen schadet der Demokratie. In dem Maße, in dem die Informationen von privaten Plattformen ausgewählt, moderiert (bzw. manipuliert) werden, wie z. B. heute schon bei Google und Facebook, wird die politische Meinungsbildung durch Privatkonzerne in einer Weise gesteuert, die die von Medienkonzernen der „alten Welt“ weit übertrifft.

Wir brauchen daher neue Schutzdämme. Diese werden nicht von der Wirtschaft geschaffen, sondern es Bedarf Gesetze und Bürgerrechte, die die Souveränität der Menschen, die Demokratie und den Mittelstand schützen. Lanier wendet er sich gegen die „Kostenlos-Mentalität“. Dazu gehören auch Open-Source-Produkte wie Wikipedia usw. Auch die Netzpiraten (kostenloser Datenaustausch) haben dazu beigetragen, dass sich die Kostenlos-Mentalität ausgebreitet hat. In ihrer Ablehnung jeder staatlichen Regulierung haben sie den Sirenenservern auch noch einen Gefallen getan.

Er fordert, dass der Mensch nicht Anhängsel der Maschine/Informatik ist, sondern als etwas Besonderes betrachtet wird und dies im System implementiert wird. Er fordert eine Humanisierung des Internet („Humanistische Informationsökonomie“), bei der mit der Gleichsetzung von Mensch und Maschine aufgehört wird. Entscheidende Neuerung sollte sein, dass alle Daten doppelt verknüpft sind. Links müssen also immer in beide Richtungen weisen, so dass man bei allen Dokumenten stets rückverfolgen kann, woher die Daten/Informationen stammen. Dies würde es ermöglichen, dass Informationen stets einen kleinen Betrag kosten, wenn sie genutzt werden. Damit würde die Kostenlos-Mentalität beendet.

Jeder hätte ein Grundrecht auf seine Daten. Jede Benutzung – bzw. Verlinkung – müsste vergütet werden. Dies könnte vollkommen automatisch im Netz stattfinden – also quasi im Netz implementiert werden. Benutzer müssen wechseln können und ihre Daten und Kontakte mitnehmen. Dazu muss jeder Mensch im Netz eine eigene Identität besitzen. Diese soll entweder vom Staat vergeben werden wie ein Personalausweis, oder der Staat regelt die Vergabe durch Gesetze (allgemeine User-ID). Informationen müssen grundsätzlich zwischen allen Netzen ausgetauscht werden können. Das bedeutet, dass Mitteilungen z. B. von einem Facebook-Nutzer grundsätzlich an meine Identität – also an mich – weitergeleitet werden müssen, egal in welchem Netz ich mich befinde. Das bedeutet, dass alle Systeme offen sein müssen. Wenn ich bei Facebook kündige, dann bekomme ich alle Kontaktdaten ausgehändigt und kann diese weiter nutzen, wenn ich zu einem anderen Provider wechsle (Karl-Martin Hentschel, Kiel).

Monika Kuschewsky (Hrsg.)
Data Protection & Privacy, 3rd Edition
Thomson Reuters, London, 2016
ISBN 9780414057333
240 GBP/ 440 EUR

(ks) Bereits die vorhergehende Ausgabe dieses englischsprachigen Werks wurde in der DANA 2/2015 besprochen. Seit damals ist das Werk vermutlich auch in Deutschland etwas bekannter geworden. Jedenfalls führt es der Online-Buchhändler, der fast alles beschafft, inzwischen auch im Sortiment – allerdings nur über einen japanischen Anbieter vermittelt. Allein der stolze Preis, den es für den Erwerb hinzublättern gilt, verhindert vermutlich weiterhin die flächendeckende Verbreitung bei Praktikern, die diesem Werk eigentlich zu wünschen wäre.

Denn für alle Datenschützer, die nicht ausschließlich deutsche Kunden

betreuen (und davon gibt es immer weniger), stellt dieses Werk ein äußerst komfortables Portal zur Datenschutz-Rechtslage in vielen Teilen der Welt dar. Nicht unter Mühen und mehr oder weniger erfolgreich im Internet nach Datenschutzgesetzen aus aller Welt suchen zu müssen, ist das große Verdienst von Monika Kuschewsky und ihren Ko-Autoren.

Die dritte Auflage deckt 46 Jurisdiktionen aus sechs Kontinenten ab und gibt damit erneut über mehr Länder als die Vorauflage Auskunft. Außerdem sind wiederum Zusammenfassungen für die Regionen Asien-Pazifik und Lateinamerika enthalten. Leider muss man allerdings feststellen, dass den zwölf Neuzugängen (Bulgarien, Kanada, Costa Rica, Hong Kong, Ungarn, Luxemburg, Marokko, Russland, Serbien, Südafrika, Südkorea, Arabische Emirate) vier Länder gegenüberstehen, die in der neuen Auflage nicht mehr erscheinen. Dass hierzu ausgerechnet Indien gehört, das eine ganz besondere Rolle beim Outsourcing vieler großer Unternehmen spielt, ist nicht nachvollziehbar. Was auch immer zu dieser Entscheidung geführt haben mag: Dieser Verzicht ist außerordentlich bedauerlich.

Der Nutzen bezüglich der bearbeiteten Länderjurisdiktionen ist allerdings enorm: Nach einem übersichtlichen und immer gleichen Schema beschreiben die Autoren die jeweilige Datenschutz-Rechtsgrundlage, ihren Anwendungsrahmen, die aufsichtsbehördlichen Strukturen, wesentliche Verarbeitungsprinzipien (genauer auch in besonders relevanten Bereichen wie Beschäftigtendaten, Gesundheitsdaten, Finanzdaten, Telekommunikationsdaten u.a.), Informationsrechte und -pflichten, Anforderungen an Outsourcing, IT-Sicherheitsanforderungen, Audits, Rahmenbedingungen für Datenschutzbeauftragte und Haftungs- und Sanktionsregeln. Dieses Vorgehen erleichtert nicht nur die Überblicksgewinnung sondern auch die schnelle Vergleichbarkeit von Ländern. Aktuelle Aspekte wie Cloud Computing, Big Data, Privacy Impact Assessment und die neue EU-Datenschutzgesetzgebung haben ebenfalls Eingang in die Betrachtungen gefunden.

Das Werk stellt damit weiterhin für Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Compliance Officer, Konzernbetriebsräte und sonstige, mit internationalem Datenverkehr befasste Personengruppen eine in höchstem Maße wertvolle Quelle strukturierter Erstinformation dar. Ihm wäre zu wünschen, dass einmal aufgenommene Länder nicht ohne erkennbaren Grund entfallen und die Länderliste kontinuierlich erweitert wird.

Ein attraktiverer Preis wäre sicherlich hilfreich, für die verdienstvolle und offensichtlich arbeitsintensive Darstellung eine weit größere Lesergruppe zu gewinnen. Dazu sollte auch der Vertrieb über den Buchhandel und den Online-Buchhandel ermöglicht werden.



Fabian Siegler
Die Datenschutz-Lüge
ISBN 978-3-7345-6963-0, tredition, 25,99 €

Christina Körner: **Datentracker – Webtracking und Datenschutz im Jahr 2016**

(ck) Ob Cookies, Tags, Web-Bugs, Pixel, Fingerprinting oder Web-Beacons – durchschnittlich lesen 75 Web-Technologien bei einem Webseitenaufruf mit. Durch Webtracking werden viele User mehr und mehr zum ‚gläsernen Menschen'. Und das ohne ihr Wissen.

„Mit diesem Buch möchte ich dazu beitragen, dass Nutzer für das Thema Datentracking sensibilisiert werden und ihre Surfgewohnheiten überdenken", sagt Fabian Siegler, Marketing-Experte für Echtzeit-Personalisierung. Denn Millionen und Milliarden Nutzerdaten werden täglich gesammelt. Nicht nur der Suchmaschinengigant Google, auch Facebook, Amazon & Co. schöpfen die Daten der Nutzer ab. Der Autor prangert nicht den Datenschutz an, verfasst auch keinen neuen Enthüllungsreport. Er wird in seiner täglichen Praxis mit der digitalen Datenerhebung konfrontiert und weiß, wovon er redet, wenn er sagt: „Nicht alles, was legal ist, ist auch sinnvoll."

Fabian Siegler plädiert für mehr Aufklärungsarbeit und möchte mit diesem Titel dazu beitragen, für mehr Transparenz beim Webtracking zu sorgen: Zuerst werden in dem rund 500 Seiten starken Buch die Entwicklungen der Echtzeit-Personalisierung und die ständig steigende Datenflut, die uns täglich umgibt, beschrieben. Er möchte neue Einsichten schaffen, so dass ‚Otto-Normal-User' sieht, wo ‚unsere' Daten täglich verarbeitet und verwertet werden. „*... Es darf nicht vergessen werden, dass aufgrund der Schnelllebigkeit Kampagnen heute immer öfter optimiert werden (müssen). Nur durch fortlaufende Anpassungen ist es möglich, dem ständigen Wettbewerbsdruck und natürlich auch den Interessen der Nutzer gerecht zu werden. Ebenfalls auf dem Vormarsch ist das sogenannte Realtime-Advertising. Letzteres ermöglicht das Buchen von Werbeflächen in Echtzeit. Da dies im Bereich von Millisekunden geschieht, ist neben einer guten Infrastruktur vor allem eines nötig: Daten! Aktuelle Daten ...*" (Auszug aus dem Buch Datentracking von Fabian Siegler)

Der Autor schaut über den Tellerrand und macht anhand von Beispielen aus der Praxis deutlich, inwieweit unsere Datenspuren, die wir unbewusst verursachen, sich zu einer Einheit zusammenführen lassen. Es zeigt sich, dass dabei Parameter wie Aufenthaltsort, Tageszeit, Point of Interest, Computer-ID und Haushaltsdaten von entscheidender Bedeutung beim Datensammeln sind und beim Website-Login das Profil und die Identität des Users dann gänzlich deckungsgleich werden.

Für den Leser wird nachvollziehbar, was das Datensammeln bewirken kann: Ob es sich dabei um Ortungsdaten im öffentlichen Verkehr handelt – das sogenannte Geo-Targeting – oder die Standortfreigabe, der derzeit 67 Prozent der Smartphone-User ganz selbstverständlich zustimmen. Wie der User mit dem scheinbar harmlosen Spiel Pokémon Go zahlreiche Umgebungsdaten sammelt und wer dahinter steckt, so dass die sensiblen Daten problematisch werden können und dass das Spiel in Russland und im Iran gar nicht erlaubt ist. Wie abhängig wir vom Smartphone sind, zeigt das Beispiel mit dem spanischen Strand, der

nur online gebucht und offline besucht werden kann. Auch der Zusammenhang von vernetzter Kleidung macht die Vor- und Nachteile nachvollziehbar: Die Daten der Kleidung werden zum Smartphone gesendet, um uns vor Sonnenbrand zu schützen, aber klar ist auch, dass hier noch andere Daten „abgeschöpft“ werden können. Welche Daten bei Googles Übersetzungstool erhoben werden, warum die Flugsicherheit an so scheinbar banalen Dingen wie der Menüwahl im Flugzeug nach USA interessiert ist, oder wie wir unsere Körperdaten weitergeben und die Krankenkassen davon profitieren, kann hier nachgelesen werden.

„*... Neben PC und Smartphone sind inzwischen auch eine Fülle weiterer Geräte mit Kommunikations- und somit Tracking-Funktionen ausgestattet. Bekannteste Beispiele sind etwa biometrische Sensoren für sportliche Aktivitäten, Satellitennavigationssysteme, automatische Mautzahlungssysteme und elektronische Fahrkarten für den öffentlichen Nahverkehr (Internet der Dinge). Auch die Kommunikations-, Ortungs-, und Datenverarbeitungssysteme in Kraftfahrzeugen werden weiter zunehmen, nicht zuletzt aufgrund der derzeit steigenden Nachfrage nach Car-Sharing. Durch das Auto (das mit Fremden geteilt wird) werden wieder einmal Daten – persönliche, versteht sich – benötigt. Und ja, diese werden nicht nur innerhalb der offiziellen Betreiberwebseiten bzw. Apps erhoben. Standortdaten sind wohl eine der wichtigsten Erkenntnisse, immerhin muss in Echtzeit die Warenverfügbarkeit ermittelt werden. Ebenfalls nicht zu unterschätzen ist die geplante, flächendeckende Verbreitung des sogenannten eCall-Systems. Letzteres sieht gemäß einem Vorschlag der Europäischen Kommission und des Parlaments ab dem Jahr 2015 ein Einbau in alle neuen Personenkraftwagen vor. Bewegungsprofile sind stets gefragte Daten. Ob PKW, Smartphone oder bei Google - Daten werden überall im Hintergrund erhoben. Doch das größte Problem ist wohl die Fusion sämtlicher Daten. Es ist kaum möglich, auch nur ansatzweise zu ermitteln, wo welche Daten erhoben bzw. tatsächlich verarbeitet werden. Der Weiterverkauf von Daten ist ebenfalls oftmals an der Tagesordnung. Trotzdem entsteht dank der fortschrittlichen Digitalisierung erhebliches Potenzial. Ein fast abzusehender Nebeneffekt, der mit dem beschriebenen eCall-System einhergeht, ist die rasante Verbreitung solcher Plattformen. Letztere ermöglichen dann nicht nur Notrufdienste, sondern auch andere, neuartige Mehrwertdienste. Eine Möglichkeit sind individuelle Versicherungsbeiträge, ähnlich wie es gerade im Gesundheitswesen erprobt wird. Die künftigen Fahrzeugversicherungsbeiträge könnten sich dann anhand neuartiger Parameter ermitteln lassen, wie etwa die Fahrleistung. Natürlich erfolgen derartige Analysen auch unter Berücksichtigung der gewählten Strecken sowie des Verhalten des Fahrers. Beispiele für das Fahrerverhalten sind überdurchschnittlich häufiges Beschleunigen und Bremsen. Auch könnte der Mindestabstand zum Vordermann oder das Überfahren von roten Ampelanlagen mögliche Parameter für ein Nutzerprofil sein. Wenn die Systeme tausendfach in Betrieb sind, ergeben sich riesige Vergleichsdatenbanken. Eben solche, die man bislang vorwiegend Google und Co. anlastet ...*“

Mit diesem Buch wurde für den Leser eine Grundlage geschaffen, sich mit den möglichen Einsatzgebieten der Website-Tracker, deren Risiken aber auch mit deren Potenzial vertraut zu machen. Dafür wurden rund 185 Daten-Tracker detailliert analysiert und beschrieben.

Auf den Name des Programms und des Anbieters folgt die Internetseite des Anbieters und der Direktlink zu den Datenschutzinfos. Außerdem wird beleuchtet, wie die Daten erhoben werden, das PlugIn Ghostery bildete die Grundlage für die Aufzählung der Informationen. Es folgt die Recherche ob Data Sharing betrieben wird und der Datenschutz-Kontakt wird aufgeführt. Es wird deutlich, wann die Tracker entstanden sind, welche Funktion sie haben und von wem sie eingesetzt werden. Sehr interessant ist jeweils der Firmensitz, denn er entscheidet maßgeblich über die damit verbundenen Datenschutzgesetze, denen sich die Firmen verpflichtet fühlen oder wo sie zertifiziert wurden.

Rund 50 Screenshots von 50 Webseiten zeigen alle zum Zeitpunkt der Überprüfung gefundenen Tracker. Die Webseiten wurden anhand der SEO-Toolbox SISTRIX Tool Top 100 ermittelt und die Auswahl ist nicht wertend. Sie deckt eine breite Palette an Kategorien und Themen der Unternehmen ab. Auf jedem Screenshot ist rechts im Bild eine „Lila Liste“ zu finden. Dort sind eben jene Anbieter und Tracker zu finden, die in einem Verzeichnis nachgeschlagen werden können. Außerdem ist eine Kurzbeschreibung jeder überprüften Website gemacht worden. Danach hat der Autor explizit die Datenschutzbeauftragten der einzelnen Webseiten angeschrieben und sie zu den auf ihren Webseiten gefundenen Hintergrundprogrammen befragt. Es handelt sich um die immer gleichen Fragestellungen. Rund die Hälfte der Webseitenbetreiber hat zu den zehn Fragen keine Stellung bezogen, oder mit vorgefertigten Antwort-Mails operiert. Es waren nur sehr wenige Unternehmen dabei, die sich persönlich und detailliert zu den Programmen geäußert haben. Aus Datenschutzgründen wurde auf die Personen- oder Mitarbeiter-Namensangabe bei Anfragen-Feedbacks verzichtet. „Ich habe das Gefühl gewonnen, dass mir aus Unwissenheit heraus nicht geantwortet wurde. Ich vermute, viele – oft kleinere – Unternehmen sourcen die Gestaltung ihrer Webseite aus. Und die jeweilige Agentur, die das Webseiten-Projekt dann betreut, lädt Verschiedenes drauf, was wiederum die Webseitenbetreiber gar nicht erklären können“, glaubt der Marketingexperte.

Welchen Zusammenhang die Tracker mit der Ladezeit der einzelnen Websites bilden und was das über die Glaubwürdigkeit der Unternehmen aussagt, wird ebenfalls anhand von Screenshots gezeigt. Im letzten Kapitel geht es dem Autor darum, dem Nutzer Wege aufzuzeigen, wie er Scripte blockieren und wie er seine persönlichen Daten schützen kann. Welche Programme Vor- und Nachteile für seine persönlichen Bedürfnisse bieten und wie er mit speziellen Tools bewusst die Privatsphäre-Einstellung steuern kann. Denn bis zum Jahr 2017 erwartet Google, dass rund 37.000 GB pro Sekunde an Daten verarbeitet werden. Allerhöchste Zeit, sich über die Sicherheit und Nutzung der Daten Gedanken zu machen.

„Ich denke, dass noch viel Aufklärungsarbeit notwendig ist, und selbst Leute, die für die Webseiten zuständig sind, haben nur bedingt Ahnung von Webtracking“, vermutet der Autor Fabian Siegler.


RECHT AUF PRIVATSPHÄRE
WIR SCHAFFEN DAS AB
„Das Prinzip der Datensparsamkeit kann nicht die Richtschnur sein für die neuen Produkte“
HAT SIE NICHT EINMAL GESAGT: „ABHÖREN VON FREUNDEN, DAS GEHT GAR NICHT“?
JA, DARAUS GEHT ABER NICHT HERVOR, DASS DIE BEVÖLKERUNG DEUTSCHLANDS ZU **IHREN** „FREUNDEN“ GEHÖRT!
© 2016 Frans Valenta